SİBER OLAY ALGORİTMASI ÜZERİNE

SELÇUK DİKİCİ
ENDÜSTRİ MÜHENDİSİ

Siber Olay Nedir?

Siber olay, bir bilgi süreci, ağda veya dijital bir ortamda gerçekleşen, güvenlik politikalarını, kullanımlardan veya faaliyetlerin bilgi güvenliği parametrelerinin kesintiye uğradığı bir durum veya olaydır. Bu tür olaylar, güvenlik açıkları, tehditler, saldırılar veya teknik arızalar sonucu ortaya çıkabilir ve bilgi sistemlerinde yetkiliz erişim, veri sızıntısı, hizmet kesintisi gibi zararlara yol açabilirsiniz.

Siber Olayın Türleri:

1. **Yetkisiz Erişim:**
    - Bir veya kişilerin saldırganın, izni olmadan bir sistem veya erişim erişim sağlama durumudur. Bu, güvenlik açığı olan sistemlerde veya zayıf parola kullanımında genel talimatlar bir olaydır.
2. **Veri Sızıntısı:**
    - Hassas veya gizli bilgilerin yetkisiz kişiler tarafından elde edilmesi, bir siber olaydır. Bu, bir güvenlik açığı sonucu veya saldırı sonucu olabilir.
3. **Zararlı Yazılım (Kötü Amaçlı Yazılım) Saldırıları:**
    - Virüs, solucan, truva atı gibi zararlı yazılımlar sistemlere bulaşarak veri çalabilir, sistemleri bozabilir veya şifreleyerek fidye talep edebilir.
4. **Hizmet Reddi (DoS/DDoS) Saldırıları:**
    - Bir sistemi veya hizmeti aşırı trafikle yükleyerek erişilemez hale getirme olayıdır. Bu tür saldırılar, organizasyonların bozulmasına neden olur.
5. **İç Tehditler:**
    - Bir Organizasyonun içindeki yetkili kişilerin, yetkilerini kullanarak bilgi sistemlerine zarar verme, veri sızdırması veya sabotaj yapmasıdır.

Siber Olayın Etkileri:

- **Finansal Zarar:** Siber olaylar, veri hırsızlığı veya hizmet kesintisi gibi koşullar nedeniyle organizasyonların gelir kaybına neden olabilir.
- **İtibar Kaybı:** Bir siber olay, müşteri verilerinin çalınması veya sistemlerin hizmet verememesi nedeniyle bir yardımın itibarını ciddi şekilde zedeleyebilir.
- **Yasal Sonuçlar:** Özellikle kişisel verilerin kesilmesi durumunda, organizasyonlar büyük yasal cezalarla karşı karşıya kalabilirler (örneğin, KVKK veya GDPR cezaları).
- **Operasyonel Kesinti:** Siber olaylar, organizasyonların iş süreçlerini kesintiye uğratabilir ve aksamalara neden olabilir.

Siber Olaylara Örnekler:

1. **Facebook Veri İhlali (2018):**
    - 50 milyon kullanıcı hesabının ele geçirildiği büyük bir veri sızıntısı olayı yaşanmış ve kullanıcı bilgileri Saldırganlar tarafından çalınmıştır.
2. **WannaCry Fidye Yazılımı (2017):**
    - Dünyadaki binlerce bilgisayardaki bir fidye yazılım saldırısıdır. Zararlı yazılım, kullanıcıların bilgisayarlarını şifreleyip çözmek için fidye talebinde bulunmuştur.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

3. **Equifax Veri İhlali (2017):**
    - ABD'de büyük bir kredi raporlama ajansı olan Equifax'ta yaşanan verinin sonucu, 147 milyon kişinin kişisel ve finansal bilgileri çalındı.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

Siber Olaylara Karşı Tedbir Almanın Amacı

Siber olaylara karşı önlem almanın temel amacı, bir desteğin bilgi altyapısı altyapısını koruyarak sistemlerin güvenli, sürekli ve etkili bir şekilde çalışmasının sağlanmasıdır. Siber olaylar, veri kesintileri, sistemin çökmesi, hizmet kesintileri ve kayıplar gibi ciddi yaralanmalara yol açabilir. Bu nedenle proaktif önlemler siber güvenlik sistemlerinin önemli bir parçasıdır.

Siber Olaylara Karşı Tedbir Almanın Başlıca Amaçları:

1. **Veri Gizliliği:**
    - Bilginin ve yetkisiz erişimin korunması esastır. Özellikle müşteri bilgileri, ticari sırlar ve kişisel bilgiler gibi hassas bilgiler korunmazsa ciddi zararlar ortaya çıkabilir. Siber güvenlik düzenlemeleri, bu tür verilerin yalnızca yetkili kişilerce erişilebilir olmasını sağlar.
2. **Veri Bütünlüğü Sağlama:**
    - Bir sistemdeki paranın korunmasının ve korunmasının korunması, siber güvenlik önlemlerinin önemli bir amacıdır. Verilerde yapılacak yetkisiz değişiklikle
3. **Sistemlerin eritilebilirliği Sağlama:**
    - Sistemlerin sürekli bir şekilde çalışması, özellikle e-ticaret, finans ve kamu hizmetleri gibi sektörler için hayati öneme sahiptir. Hizmet Reddi (DoS) saldırıları gibi siber olaylar, sistemlerin kullanılabilmesi
4. **İş Sürekliliğinin Sağlama:**
    - Bir siber olay durumunda, iş parçacıklarının kesintiye uğraması ya da minimum etkilenmesi için önceden izlenmesi sağlanır. Bu, yedekleme sistemleri, felaket kurtarma planları ve siber olay müdahale planlarının mevcut olmasıyla sağlanmıştır. Amaç, herhangi bir saldırı veya bozulmadan sonra hızla toparlanmak ve şeyin sürekliliğini sağlamaktır.
5. **İtibarın Korunması:**
    - Siber olaylar, bir yardımın güvenlik açıklarını ortaya çıkarıyor ve müşteri güvenini ciddi anlamda sarsabilir. Müşteri bilgileri veya ticari sırların ifşa olması, bir şirketin itibarını olumsuz etkileyebilir. Bu nedenle siber güvenlik prosedürleri, organizasyonların itibarını korumak için kritik öneme sahiptir.
6. **Yasal ve Düzenleyici Uyumluluk:**
    - Birçok ülkede veri koruma ve bilgi güvenliğiyle ilgili katı düzenlemeler ve kurallar bulunmaktadır. Örneğin **Kişisel Verilerin Korunması Kanunu (KVKK)** ve**Genel Veri Koruma Tüzüğü (GDPR)** gibi düzenlemeler, bunların veri koruması ve Gizlilik ihlaline uymaması zorunludur.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

7. **Maddi Kayıpları Önleme:**
    - Siber saldırılar, organizasyonlara finansal açıdan büyük zararlar verebilir. Bir veri durumundaki organizasyonlar, itibar

Siber Olaylara Karşı Alınabilecek Başlıca Tedbirler:

1. **Güçlü Parola Politikaları:** Zayıf parolalar, saldırganların sistemlerine kolayca erişim sağlanmasına neden olabilir. Güçlü parolaların kullanımı ve iki faktörlü kimlik doğrulama gibi ek güvenlik katmanları, saldırılara karşı koruma sağlar.
2. **Güncel Yazılım ve Sistemler:** Yazılım ve sistemlerin düzenli olarak güncellenmesini, güvenlik açıklarının kapatılmasını sağlar. Güncel olmayan yazılımlar, saldırganların yararlanabileceği güvenlik açıkları oluşturur.
3. **Ağ Güvenliği:** Güvenlik duvarları, Saldırganların ağa yetkisiz erişim sağlamasını önler. Ayrıca, ağ şeması sürekli izlenerek anormallikler tespit edilerek yeniden değiştirilebilmektedir.
4. **Eğitim ve Farkındalık Programları:** Çalışanların siber güvenl
5. **Sızma Testleri (Penetrasyon Testleri):** Organizasyonların siber güvenlik açıklarını tespit etmek ve bu açıkları kapatmak için düzenli olarak s
6. **Yedekleme ve Felaket Kurtarma Planları:** Önemli verilerin düzenlenmesi

***Siber olaylara karşı işlem almak, bir kutlamanın kaydedilmesini, kişisel verilerin bütünlüğünü ve sistemlerin erişilebilirliğini sağlamak için**

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

Siber Olayın Suçla İlişkilendirilmesi

Siber olaylar, dijital sistemlerde yaşanan, güvenlik açıklarının kullanılması veya sistemlerin genişlemesinin kullanılmasıyla meydana gelen olaylardır. Bu tür olaylar, çoğu zaman yasadışı suç teşkil edebilir ve çeşitli yasa dışı eylemlerle ilişkilendirilebilir. Siber olaylarla ilgili olarak, bir kasıtlı olarak yasa dışı olarak gerçekleştirilmesiyle ya da mevcut yasal düzenlemelerin ilerlemesi sonucu oluşur. Teknolojinin ve dijital sistemlerin yaygınlaşmasıyla birlikte, siber suçlar da küresel bir tehdit haline geldi.

Siber Olayı ve Siber Suç Arasındaki İlişki

Siber suçlar, doğrudan dijital sistemler üzerinde gerçekleşen ve genellikle kasıtlı bir şekilde zarara yol açmayı hedefler. Siber olaylar, birçok farklı türde yasa dışı faaliyetle ilişkili olabilir. Bu tür olaylar, bireysel kullanıcılardan büyük şirketlere ve hatta devletlere kadar geniş bir yelpazede zararlara yol açabilir.

1. Yetkisiz Erişim ve Suç İlişkisi

- **Yetkisiz erişim** , bir kişi ya da grup, bir sistem bilişim veya ağa yetkisi olmadan girilmedir. Yetkisiz erişim, suç olarak kabul edilir çünkü bu eylemin gizliliği ihlal edilir ve kurbanın sistemlerine, sistemlere veya diğer dijital varlıklara zarar verilebilir.
- **Türk Ceza Kanunu (TCK) 243. Maddesi** , izinsiz erişime izin verilmeyen yasadışı bir eylem olarak kayıtlıdır. Bu durum, bir siber olay suçun elde edilmesine yol açar. Örneğin, bir hacker'ın bir bankanın veri tabanına izinsiz girmesine, veriye yönelik ve suçun yürütülmesine yol açılabilir.

2. Veri Hırsızlığı ve Gizlilik İhlalleri

- **Veri çoğalması** ve **veri hırsızlığı** , bir siber olay ve yaygın türlerdendir. Kişisel bilgilerin, ticari sırların veya kritik verilerin çalınması, gizlilik yasalarının ihlal edilmesi.
- Kişisel verilerin korunmasını sağlar, bu tür olaylar suç olarak yaşanabilir. Örneğin **Kişisel Verilerin Korunması Kanunu (KVKK)** , kişisel verilerin izinsiz olarak saklanmasına ceza verir. Bu kanun ihlalleri, genellikle büyük para cezalarına ve yasal yaptırımlara neden olur.
- **Örnek** : Bir veri sızıntısı olayı sonucu, bir şirketin müşteri bilgileri internete sızdırılırsa, bu hem bir siber olay hem de suç teşkil eder. Bu suç, genellikle para cezaları, itibar kaybı ve müşteri tazminatları içerir.

3. Fidye Yazılımı ve Şantaj Suçu

- **Fidye yazılımları** , bir bilgisayarda bulaşan dosyalar şifreler ve kullanıcılardan bu dosyaların yeniden erişilebilir hale gelmesi için talep eder. Bu, dijital şantajın en yaygın biçimlerinden biridir.
- **Suç Unsuru** : Fidye yazılım saldırıları, **şantaj** ve **dolandırıcılık** suçlarını içerir. Saldırganlar, dosyaların açılması karşılığında kurbanlardan fidye talep eder ve bu eylemlerin dışıdır. Türk Ceza Kanunu'na göre şantaj ve dolandırıcılık suçları ciddi cezalarla kaybedildi.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

4. Kimlik Hırsızlığı ve Mali Suçlar

- **Kimlik hırsızlığı** , kişisel bilgileri çalmak ve bu bilgileri sahte işlemler yapmak için kullanmaktır. Bu siber olay türü, finansal dolandırıcılık ve kimlik sahteciliği gibi suçlarla doğrudan kullanılabilir.
- **Suç Unsuru** : Kimlik hırsızlığı, bir bireyin mali işlemler yapması, kredi kartı dolandırıcılığı yapması veya sahte hesaplar açmak amacıyla kimlik bilgilerinin çalınmasıyla. Bu, suç kapsamında değerlendirilen bir eylemdir ve çoğu ülkede ağır cezalarla karşılık bulmaktadır.

5. Hizmet Engelleme (DoS/DDoS) Saldırıları ve Suç Niteliği

- **Hizmet engelleme saldırıları (DoS/DDoS)** , bir sistem veya ağın aşırı trafik yoğunluğuyla çalıştırılan hizmet veremez hale getirme işlemidir. Bu saldırılar, sunucu ve hizmetlerin kullanımına neden olur ve bu da iş kaybına, müşteri memnuniyetisizliğine ve maddi zarara yol açar.
- **Suç Unsuru** : Bu saldırılar, bunların sürekliliğini bozar ve ciddi kayıplara yol açabilir. Bu tür saldırılar birçok ülkede yasa dışı olarak kabul edilir ve ağır yaptırımlar uygulanır. TCK, bu tür siber saldırılara karşı ciddi cezalar öngörüyor.

6. İç Tehditler ve Güven İhlalleri

- **İç tehditler** , bir şirketin içindeki yetkili bir çalışanın, sahip olduğu erişim ayrıcalıklarını genişletmeyi kullanarak bilgi sızdırması, sistemlere zarar vermesi veya bilgi satmasıdır.
- **Suç Unsuru** : Ticari sırların çalınması, sabotaj veya kurumsal olarak sınıflandırılması ve hukuki olarak suç teşkil etmesi. İç tehditler, özellikle büyük kuruluşlar için ciddi bir sorun olabilir ve hem iş hem de yasal sonuçlar açısından çok tehlikelidir.

7. Oltalama (Kimlik Avı) ve Dolandırıcılık Suçları

- **Oltalama saldırıları** , bir kişinin kişisel, finansal veya gizli olarak ele geçirilmesi amacıyla sahte e-postalar veya sahte web siteleri kullanılarak yapılan dolandırıcılık türüdür.
- **Suç Unsuru** : Oltalama saldırıları, sahtekarlık ve kimlik hırsızlığı suçlarına doğrudan yol açar. Kurbanlar bu tür saldırılar sonucu maddi kayıplar yaşarlar. Sahtekarlar, oltalama yoluyla gösterge bilgilerini dolandırıcılık yapmak için kullanır, bu da yasa dışı bir eylemdir.

Siber Suçlar ve Hukuki Düzenlemeler

Siber suçların yaygınlaşması, ülkelerin bu suçlara karşı kapsamlı yasal düzenlemelerini zorunlu hale getirmesi zorunludur. Aşağıda bazı önemli düzenlemeler yer almaktadır:

- **Türk Ceza Kanunu (TCK)** : Türkiye'de bilişim sistemlerine yönelik suçlar, **243-246. maddeler** kapsamında düzenlenmiştir. Bu maddeler, bilişim sisteminin yetkisiz erişimi, veriyi bozma ve veriyi değiştirme gibi suçları kapsar.
- **Kişisel Verilerin Korunması Kanunu (KVKK)** : Türkiye'de kişisel verilerin korunması kanunu, verilerin kullanılmasına izin verilmemesi veya çalıştırılması

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

durumunda ağır cezalar getirilir. KVKK, özellikle veri ihlalleri ve veri hırsızlığı gibi olayların suç kapsamına alınmasını sağlar.

- **Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)** : GDPR, Avrupa Birliği'nde kişisel verilerin saklanmasıyla ilgili sıkı parçalar gelir. Veri ihlalleri ve gizlilik ihlalleri, GDPR kapsamında ciddi yaptırımlara tabidir. Kurumlar, GDPR'a uygun olmayan veri işleme işlemlerinde barındırdığı ağır para cezalarıyla karşı karşıya kalıyor.

Uluslararası Boyut ve İşbirliği Zorunluluğu

Siber suçlar genellikle uluslararası boyutlara sahiptir. Saldırganlar, bir ülkede suç işleyip başka bir ülkede saklanabilir ya da saldırılar, birden fazla ülkede zarar görebilirler. Bu nedenle siber suçlarla mücadelede uluslararası işbirliği kritik bir önem taşımaktadır. **Interpol** , **Europol** gibi uluslararası güvenlik kuralları, siber suçları izlemek ve yasalları adalete teslim etmek için işbirliği yapmaktadır.

Siber Suçların Önlenmesi İçin Alınabilecek Tedbirler

1. **Güvenlik Farkındalığı ve Eğitimi** : Hem siber suçlar konusunda bilinçlendirilmesi ve eğitilmesi, hem de saldırıların önlenmesi için önemlidir.
2. **Teknik Güvenlik Önlemleri** : Güvenlik duvarları, antivirüs yazılımları, güncellemeler ve şifreleme yöntemleri gibi teknik izlemeli siber saldırıların çalıştırılmasını sağlar.
3. **Yasal Düzenlemeler ve Uygulamalar**: Siber suçlara karşı caydırıcıların kullanabileceği ve siber suç tanımlamaları ile ağırlaştırılmış cezalar.

****

Siber olaylar ve suçlar arasındaki ilişki ol

Siber Olayların Suç ile İlişkilendirilmesinin Detayları

Siber olaylar

1. Siber Olayların Suç Unsurları

Siber olaylar, çoğu

2. Yasal ve Düzenleyici Çerçeveler

Siber suçla ilişkileri, dijital ortamda güvenlik tehditlerinin hem teknik hem de hukuki boyutları

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

3. Uluslararası Boyut ve İşbirliği Zorunluluğu

Siber suçlar, genellikle sınırlardaki ve uluslararası boyutlardaki suçlardır. Bir ülkelerde işlenen bir siber suç, farklı dağılımların görünürlüğü. Bu nedenle, uluslararası işbirliği siber suçlarla mücadelede kilit rol oynuyor. **Interpol** , **Europol** gibi

4. Listeler ve Kurumlar İçin Tehdit

Siber suçlar, sadec

5. Siber Güvenlik Tedbirleri ve Önemi

Siber olayla

6. Siber Suçlarla Mücadelede Hukukun Rolü

Siber suçlar,

Detaylı Sonuç ve Değerlendirme

1. **Siber Olaylar Artık Sadece Teknik Bir Sorun Değil, Hukuki Bir Meseledir:**
    - Siber o
2. **Siber Suçlar Her Geçen Gün Daha Karmaşık Hale Geliyor:**
    - Teknolojinin gelişmeleriyle birlikte siber suçlar
3. **Siber Güvenlik, Hem oranlarıı Hem de Kurumları Korumalıdır:**
    - Siber suçların doğrulanması
4. **Yasal Düzenlemeler, Siber Suçlara Karşı Çaydırıcı Rol Oynanmalıdır:**
    - Etkili yasal düzenlemeler, siber suçların
5. **Siber Suçların Önlenmesi İçin Eğitim ve Farkındalık Şartları:**
    - Siber suçların tedbiri için teknik tedbirler

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

Genel Değerlendirme: Siber Olayların Suçla İlişkilendirilmesi

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1. Siber Suçlar Karmaşık ve Küresel Bir Tehdittir

Siber suçlar,

2. Siber Güvenlik Tedbirleri, Suçların Önlenmesi İçin Kritik Rol Oynar.

Siber olayların suçla ilişkilendirilmemesi ve bu sonuçlar

3. Hukuki Düzenlemeler Siber Suçlara Karşı Çaydırıcı Olmalıdır.

Siber suçlar, yasal düzenleme çerçeveleri ele alınmalı ve caydırıcı cezalarla karşılık bulmalıdır. Türk Ceza Kanunu (TCK), Kişisel Verilerin Korunması Kanunu (KVKK) ve Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) gibi yasal düzenlemeler, siber suçlara karşı alınan önlemler arasında önemli bir yer tutar. Yasa dışı erişim, veri çıkışı, kimlik hırsızlığı gibi suçlar, bu düzenlemeler sayesinde cezai yaptırımlarla karşılaşılır.

4. İnsanların ve Kurumlar İçin Bilinçlenme Önemlidir

Siber suçların hedefinde hem bireyler hem de kurumlar vardır. Kurumlar, büyük çapta veri kesintileri ve hizmet kesintileriyle karşı karşıya kalırken, bireylerin kimlik hırsızlığı, dolandırıcılık ve oltalama saldırıları gibi suçlardan muaf olabilirler. Bu nedenle siber suçlar konusunda kalıcılık sağlamak ve eğitim programlarının düzenlenmesi önemlidir. Çalışanların ve çalışanların, temel güvenlik protokollerini bilmesi ve uygulaması, siber suçların uygulanmasında hayati rol oynuyor.

5. Uluslararası İşbirliği Gerekli

Siber suçlar genellikle uluslararası boyutlarda işlendiğ

***

Siber olayların suçla ilişkileri, siber güvenlik alanlarındaki ayrıntılar en büyük zorluklardan biridir. Teknolojik gelişmelerle

Siber Olay Müdahale Algoritması

Siber olaylara müdahale süreci için bir değiştirmek, olayın tespitinden çözüme kadar atılması gereken adımlar sistematik bir şekilde sunar. Bu adımların doğru sırayla ve doğru müdahalelerle takip edilmesi, siber saldırıların etkili bir şekilde sürdürülmesini sağlar.

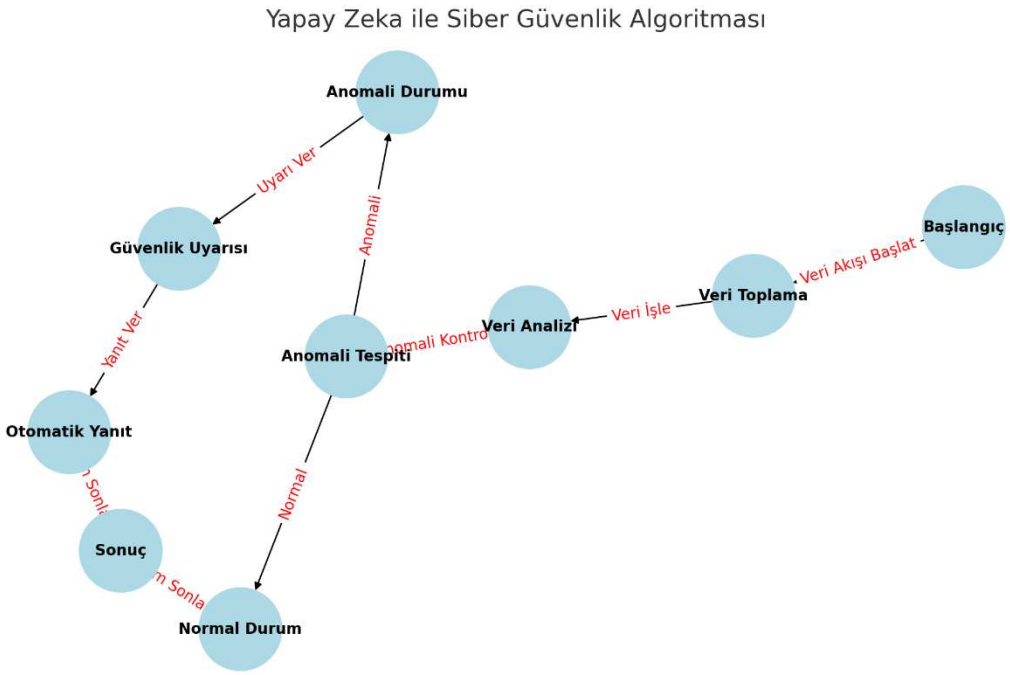
1. **Olayın Tespiti**
    - **Girdi** : İzleme araçlarından gelen anormal trafik veya sistemin devam etmesi.
    - **İşlem** : İzleme sistemlerinin gelen logları incelenir ve olası bir güvenlik merkezi tespit edilir.
    - **Çıktı** : Potansiyel güvenlik stratejisi bildirimi.
2. **Olayın Doğrulanması**
    - **Girdi** : Olayın tespit raporu.
    - **İşlem** : Güvenliğin gerçek bir tehdit olup olmadığının belirlenmesi için olay kaynağı araştırılır. Loglar ve sistem aktarımı
    - **Çıktı** : Olayın gerçek veya yan
3. **Olayın Sınıflandırılması**

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Girdi** : Yapılandırma bilgisini olayın.
- **İşlem** : Olayın türü belirlenir. (Veri kontrolü, yetkisiz erişim, DDoS saldırısı vb.)
- **Çıktı** : Olay türü ve kritiklik düzeyi.

4. **Olayın Önceliklendirilmesi**
   - **Girdi** : Olay türü ve kritikliği.
   - **İşlem** : Olayın aciliyeti ve etkisi. (Aciliyet puan tahminleri
   - **Çıktı** : Öncelik seviyesi yüksek, orta veya düşük olarak belirlenir.
5. **Olayın İzolasyonu**
   - **Girdi** : Ö
   - **İşlem** : Olayın
   - **Çıktı** : İzole edilmiş sistemler ve durdurulan sistemler.
6. **Müdahale Eylemi**
   - **Girdi** : İzole edilen sistemler ve olay raporu.
   - **İşlem** : Olayın neden olduğu hasar azaltılmaya çalışılır. Gerekli yazılım yamaları, antivirüs taramaları, sistem temizlemeleri yapılır.
   - **Çıktı** : Olayın çözüme yönelik yapılan müdahale.
7. **Kurtarma**
   - **Girdi** : Olay müdahale raporu.
   - **İşlem** : İzole edilmiş
   - **Çıktı** : Sistemlerin eski haline getirilmesi ve operasyonların yeniden başlatılması.
8. **Olay Sonrası Değerlendirme**
   - **Girdi** : Olayın çözüme u
   - **İşlem** : Olay sonrasında analiz yapılır. Olayın kök nedeni araştırılır, olayın tekrar yaşanmaması için
   - **Çıktı** : Olayların çözümü ve gelecekte benzer olayların çözümüne yönelik stratejiler.
9. **Geri Bildirim ve Düzeltici Faaliyetler**
   - **Girdi** : Olay raporu ve analiz sonuçları.
   - **İşlem** : Sistemlerdeki güvenlik
   - **Çıktı** : İyileştirilmiş güvenlik politikaları ve güncellenmiş güvenlik politikaları

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231



Algoritmanın Pseudocode (Yalancı Kod) Formatı

START

1. TespitEt(Olay)
  IF OlayTespitEdildi THEN
    2. OlayıDoğrula(Olay)
      IF OlayGerçek THEN
        3. OlayıSınıflandır(Olay)
        4. ÖncelikBelirle(Olay)
        IF OlayÖnceliğiYüksek THEN
          5. OlayıİzoleEt(Olay)
          6. MüdahaleEt(Olay)
          7. KurtarmaSüreci(Olay)
          8. OlaySonrasıDeğerlendir(Olay)
          9. GeriBildirimVeDüzelticiFaaliyet(Olay)
        ELSE
          Olayı İzlemeye Devam Et
      ELSE
        OlayYanlışAlarm
      ENDIF
  ELSE
    OlayTespitEdilemedi
  ENDIF

END

Algoritmanın Temel Aşamaları

1. **Olay Tespiti** : Güvenlik izleme araçlarıyla
2. **Doğrulama** : Olayın gerçek bir tehdit olup olmadığı
3. **Sınıflandırma** : Olayın türü
4. **Önceliklendirme**: Olayın aciliyetine göre müdah
5. **İzolasyon** : Sistemin zarar görmesini engellemek için etkilenen bölüm
6. **Müdahale** : Olayın etk

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

7. **Kurtarma** : Etkilenen sistem
8. **Özet** : O
9. **Geri Bildirim ve Düzeltici Faaliyetler**: Sonraki olay

Bu kapatma, siber olay müdahale sürecini adım adım ele alan bir yaklaşımdır ve olası bir hedefe karşı hızlı ve etkili bir yanıt sunumu sağlar. Algoritmanın her aşamada belirli girişleri ve çıkışları vardır, bu süreçte süreç kontrollü bir şekilde ilerler.

1. Olay Tespiti ve Bildirimi

1.1 İzleme ve Algılama Sistemleri

- **Güvenlik Bilgi ve Olay Yönetimi (SIEM) Sistemleri:** SIEM sistemleri, çeşitli kaynaklar (güvenlik duvarları, antivirüs yazılımları, ağ izleme araçları vb.) gelen logları toplayarak analiz eder ve potansiyel tehditleri tespit eder. Olayların değişimini yaparak anormal durumları ve güvenlik olaylarını belirler.
- **Saldırı Tespit Sistemleri (IDS)/Saldırı Önleme Sistemleri (IPS):** IDS ve IPS sistemleri, ağ izlemeleri ve bilinen tehditlere karşı sistemler tarar. IDS, saldırıları tespit eder ve bildirir; IPS ise saldırıları önleyici aksiyonlar alabilir.
- **Anormal Algılama:** Normal sistemdeki sapmalara karşı izler ve bu sapmalar tehdit olarak değerlendirilir. Makine öğrenmesi ve yapay zeka çözümleri kullanılarak daha gelişmiş anomali tespitleri yapılabilir.
- **Log Yönetimi:** Sunucular, ağ cihazları ve uygulamalardan loglar, belirli periyotlarda izlenir ve analiz edilir. Bu loglar, olası bir saldırının veya güvenlik güçlerinin işaretlerini içermez.

1.1 İzleme ve Algılama Sistemleri

Siber olaylara müdahalenin ilk aşaması olan "Olay Tespiti ve Bildirimi" kapsamında, izleme ve algılama sistemleri kritik bir rol oynuyor. Bu sistemler, ağlar, sunucular, uygulamalar ve diğer dijital varlıklar üzerinde sürekli olarak izleme yaparak anormallikleri, tehditleri ve potansiyel güvenlik ihlallerini tespit eder. Bu bölümde, çeşitli izleme ve algılama sonuçlarının nasıl gerçekleştiği ve bu sistemlerin olay tespitindeki rollerini ayrıntılı olarak incelenerek oynanmaktadır.

1.1.1 Güvenlik Bilgi ve Olay Yönetimi (SIEM) Sistemleri

Güvenlik Bilgi ve Olay Yönetimi (SIEM) sistemleri, siber güvenlikte kritik bir sorumludur ve genellikle büyük ayrılık organizasyonlarında kullanılır. SIEM sistemlerinde, ağlarda, sistemlerde ve uygulamalarda gerçekleşen çeşitli güvenlik olaylarını tespit etmek ve analiz etmek için merkezi bir platform sunar. Bu sistemler, geniş bir yelpazede güvenlik sağlayacak şekilde toplar, analiz eder ve açıklık haklarının potansiyel tehditlerini tespit eder.

1.1.1.1 Günlük Toplamı

SIEM sistemleri, çok sayıda kaynaktan gelen log düzeni toplar. Bu kaynaklar arasında güvenlik duvarları, saklananlar, anahtarlar, sunucular, veri tabanları, uç nokta cihazları, uygulamalar ve diğer güvenlik araçları bulunur. Günlük toplama, SIEM sisteminin temel işlevlerinden biridir ve birkaç farklı yerde bulunur:

- **Syslog Protokolü:** Birçok cihaz ve uygulama, log izolasyonları için Syslogünü protokolleri kullanır. SIEM sistemleri, bu protokolü koruyan logları alır ve merkezi bir depoda saklar.
- **Agent Tabanlı Toplama:** Bazı SIEM sistemleri, ajan (ajan) yazılımları kullanarak log toplar. Bu aracılar, belirli bir cihaz veya uygulama üzerinde çalışır ve bu cihazdan doğrudan logları SIEM sistemi iletir. Bu yöntem, özellikle HIDS (Host Intrusion Detection System) gibi çözümlerle entegre olarak kullanılır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **API Tabanlı Toplama:** Modern SIEM çözümleri, bulut tabanlı hizmetlerden ve uygulamalardan log toplamak için API entegrasyonları kullanılır. Örneğin bulut tabanlı bir e-posta hizmetinden log toplamak için SIEM, ilgili API'yi bu loglar aracılığıyla alabilir.
- **Doğrudan Entegrasyon:** Bazı güvenlik ürünleri ve uygulamaları, SIEM sistemleriyle doğrudan entegre olabilir. Bu entegrasyonlar, log verilerinin hızlı ve verimli bir şekilde SIEM veri aktarımını sağlar.

1.1.1.2 Log Depolama ve Yönetim

SIEM sonuçlarının topladığı log verileri, merkezi bir veri tabanında saklanır. Bu veri tabanı, logların düzenli bir şekilde bilgilerini ve genel bilgilerin erişilmesini sağlar.

- **Veri Normalizasyonu:** Farklı kaynaklardan gelen loglar, genellikle farklı formatlarda olur. SIEM sistemleri, bu logları normalleştirerek ortak bir formata dönüştürür. Bu sayede farklı kalıntıların gelen verileri kolayca karşılaştırılabilir ve analiz edilebilir hale gelir.
- **Veri Saklama Süreleri:** SIEM sistemlerinin loglarının ne kadar süre saklanacağına ilişkin politikalar belirlenir. Bu süre boyunca, yasal gerekliliklere, ortaklığın ve depolamanın saklanmasına göre düzenlenir. Uzun süreli depolama, genellikle eski verilerin arşivlenmesiyle sağlanır.
- **Veri Güvenliği:** Logların güvenli bir şekilde saklanması, yetkisiz erişimlere karşı korunması çok önemlidir. SIEM sistemleri, logların şifrelenmesi ve erişim kontrolleri arasında bu güvenliği sağlar.

1.1.1.3 Korelasyon Kuralları

Korelasyon, SIEM sonuçlarının güçlü bir birleşimidir. Korelasyon kuralları, çeşitli log olaylarını birleştirerek bir güvenlik olayının ortaya çıkmasını sağlar.

- **Kural Tabanlı Korelasyon:** SIEM sistemleri, belirli koşullar altında bir olay dizisinin bir güvenlik tehdidinin oluşturulmasını belirlemek için kural temelli erişimi kullanır. Örneğin, bir kullanıcı önce başarısızlık açma denemelerinde vardı, ardından bir sistem başarılı bir şekilde erişilmişse, bu durum bir güvenlik riski olarak değerlendirilebilir. Bu tür bakım kuralları, SIEM ödemeleri tarafından oluşturulabilir veya önceden tanımlı olarak yapılabilir.
- **İstatistiksel Korelasyon:** SIEM sistemlerinde, normal dağılım gösteren analiz yöntemleri kullanılarak ve bunlardan kaynaklanan sapmalar tespit edilebilir. Örneğin, belirli bir IP'den gelen düzeyde yüksek sayıda istek, bir saldırı belirtisi olabilir.
- **Zaman Temelli Korelasyon:** Bu türdeki gelişmeler, olayların zaman aralığını göz önünde bulundurarak analiz yapar. Örneğin, belirli bir zaman diliminde gerçekleşen çok sayıda kesinti oturum açma denemesi, hemen ardından gelen başarılı bir oturum açma ile birleştirildiğinde, bu bir kaba kuvvet saldırısı işaretlenebilir.

1.1.1.4 Gerçek Zamanlı İzleme ve Alarm Üretme

SIEM sistemleri, topladıkları logları gerçek zamanlı olarak analiz eder ve açıklama kuralları esas alınarak anlık uyarılar oluşturur. Gerçek zamanlı izleme, tehditlerin hızla tespit edilmesi ve değiştirilmesini sağlar.

- **Uyarı Yönetimi:** SIEM sistemleri, tespit edilen olaylara göre farklı seviyelerde uyarılar üretir. Bu uyarılar, kritik düzeydeki tehditlerden (örneğin, yetkiliz veri sızıntısı) düşük bölgesel olaylara (örneğin, kullanıcıların yanlış parola girebilmesi) kadar değişebilir. Uyarılar, e-posta, SMS, anlık mesajlaşma araçları veya SIEM'in Dashboard'u üzerinden güvenlik ekibine iletilir.
- **Olay Önceliklendirme:** SIEM sistemlerinde üretilen uyarıların önem derecesine göre parlaklaştırılmasını sağlar. Bu, güvenlik ekiplerinin en kritik olaylarına kapsamlı olarak müdahale edilmesine olanak tanır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Otomatik Müdahale:** Gelişmiş SIEM sistemleri, belirli tehditler için otomatik müdahale özelliklerini sunabilir. Örneğin, bir saldırı tespit durumunun otomatik olarak ilgili IP adresinin engellenmesi gibi.

1.1.1.5 Raporlama ve Analiz

SIEM sistemlerinde, yalnızca olayların tespiti ile kalmaz, aynı zamanda bu olaylar hakkında ayrıntılı raporlar üretilir. Bu raporlar, güvenlik oranlarının, ortaya çıkışının kökenini ve değiştirilen güvenlik stratejilerinin yayılması için kullanılır.

- **Günlük ve Haftalık Raporlar:** SIEM sistemleri, düzenli olarak günlük veya haftalık raporlar üreterek sistemler ortaya çıkan özet raporlarını sunar. Bu raporları, güvenlik ekiplerinin düzenli olarak sistem bakış açısıyla gözden geçirmesine olanak tanır.
- **Olay Analizi Raporları:** Esnek bir güvenlik süreci hakkında ayrıntılı bir rapor oluşturulabilir. Bu raporlar, olayın nasıl gerçekleştiğini, hangi sistemlerin değiştirildiğini ve alınan müdahale önlemlerinin detaylandırılmasını sağlar.
- **Trend Analizi:** SIEM sistemleri, zaman içinde tekrarlayan olayları ve anormallikleri analiz ederek uzun vadeli güvenlik özelliklerini belirler. Bu analizler, tehditlerin daha iyi öngörülmesine yardımcı olur.
- **Yasal ve Uyumluluk Raporları:** Bazı endüstrilerde, belirli güvenlik gereksinimlerine uyum sağlanıyor (örneğin, PCI DSS, GDPR). SIEM sistemleri, bu tür yasal gereklilikleri karşılamak için uygun raporlar üretebilir.

SIEM (Güvenlik Bilgileri ve Olay Yönetimi) sonuçlarının en önemli işlevlerinden biri, topladığı verilerden anlamlı sonuçları çıkarmak ve bu sonuçların organizasyonunun farklı düzeydeki sürümlere iletilmesidir. Raporlama ve analiz süreçleri, hem günlük operasyonların kaydedilmesi hem de uzun vadedeki derleme kararlarının toplanması için kritik bilgilerin sağlanmasını sağlar. Bu bölümde SIEM analizleri ve analizleri ayrıntılı olarak incelenir.

1.1.1.5.1 Günlük ve Haftalık Raporlar

SIEM sistemleri, sistemin genel sonuçları ve güvenlik olaylarını özetleyen günlük ve haftalık raporlar üretir. Bu raporlar, sistem korumasıne ve güvenlik gruplarına, ağın sağlık ve güvenlik hakkında genel bir bakış sunar.

- **Günlük Raporlar:** Her günün sonunda, SIEM sistemi, o gün boyunca tüm güvenlik olaylarını özetleyen bir rapor oluşturur. Bu raporlar, tespit edilen tehditleri, alınan aksiyonları ve herhangi bir açıkta olan güvenlik zafiyetlerini içerir.
    - **İçerik:** Günlük raporlar, belirli bir gün boyunca meydana gelen tüm olayları, olay türlerini (örneğin, başarısız oturum açma denemeleri, güvenlik duvarında engellenen IP adresleri), olayların zaman değişimlerini ve kritik olaylar için alınan eylemleri içerir.
    - **Kullanım:** Güvenlik ekipleri, bu raporları inceleyerek anormal bir durumun olup olmadığını kontrol eder ve gerekirse hemen müdahale eder.
- **Haftalık Raporlar:** Haftalık raporlar, bir hafta boyunca ortaya çıkan tüm güvenlik olaylarının daha geniş bir özetini sunuyor. Bu raporları, haftalık eğilimleri ve genel sistem bilgilerini analiz etmek için kullanılır.
    - **İçerik:** Haftalık raporları, hafta boyunca meydana gelen olayların özetini, bu olayların hangi sistemleri veya ağ bölümlerini sınırlandırdığını, sık sık tehdit tehdit türlerini ve genel olarak güvenlik durumu hakkında özet bilgileri içerir.
    - **Kullanım:** Haftalık raporları, yönetim düzeyindeki karar vericilere ve CISO gibi güvenlik çözümlerine genel bir güvenlik değerlendirmesi sunar. Bu raporlar, indirgemek parçaları almak için temel oluşturur.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1.1.1.5.2 Olay Analizi Raporları

Bir güvenlik olayı hakkında ayrıntılı bilgi sağlamak amacıyla bu raporlar, kayıtların tüm ayrıntıları analiz edilir ve bu analizleri belgeleyerek gelecekte benzer olayların önlenmesine yardımcı olur.

- **Olayın Tanımlanması:** Olay analizi raporu, olayın ne olduğu, nasıl tespit edildiği, hangi sistemler veya veri varlıklarının değiştiğini ve olayın zamanının değişebildiğini.
    - **İçerik:** Rapor, olayın başlangıç noktası, saldırı yöntemi (örneğin, phishing, DDoS, kötü amaçlı yazılım), saldırının tespit edilmesi ve analiz analizi ayrıntılı olarak ele alınır.
    - **Kullanım:** Bu raporlar, olayın nasıl gerçekleştiğini ve gelecekteki benzer olayların belirlenmesi için güvenlik birimleri tarafından nasıl önlenebileceği kullanılır.
- **Kök Neden Analizi:** Olayın meydana gelmesine neden olan temel nedenleri belirler. Bu, zayıf güvenlik politikaları, insan hataları, teknik zafiyetler gibi kapsamların birleştirilmesi.
    - **İçerik:** Kök neden analizi, olayın meydana gelmesine katkıda bulunan her bir faktörün ayrıntılandırılması. Örneğin, bir veri sızıntısı olayı analiz ediliyorsa, saldırganın sistemlerine nasıl erişim oranları, hangi güvenlik kontrollerinin atlandığı ve olayın nasıl fark edilmediği gibi unsurlar incelenir.
    - **Kullanım:** Bu analiz, güvenlik politikalarını ve prosedürlerini yaygınlaştırmak için bir temel sağlar ve güncel güvenlik stratejilerini şekillendirir.
- **Etkilerin Değerlendirilmesi:** Şirketin üzerini finansal olarak, parasal ve itibar durumlarını analiz eder. Bu, olayın genel maliyeti ve risklerini anlamanın yardımcı olur.
    - **İçerik:** Etki değerlendirmesi, veri kaybı, sistem kesintisi, müşteri güveni kaybı ve yasal sonuçlar gibi faktörler içerir. Ayrıca olayın bir tamamlayıcı kurum tarafından incelenme olasılığı da değerlendirilebilir.
    - **Kullanım:** Bu raporlar, üst düzey yöneticilere ve yönetim kuruluşuna, olayın şirkete ait toplam maliyet hesaplamaları için sunulur. Ayrıca sigorta kesintileri ve yasal savunmalar için de kullanılabilir.

1.1.1.5.3 Trend Analizi

SIEM sistemleri, uzun vadeli güvenlik bilgilerini analiz etmek için büyük veri setlerini inceleyebilir. Bu analizler, sistemdeki düzenli döngüyü ve sapmaları belirleyerek, bölgedeki olası tehditleri öngörmeye yardımcı olur.

- **Olay Frekansı:** esnek olay türlerinin zamanının düzenli olarak analiz edilmesini sağlar. Bu, belirli bir saldırı bölümünde artıp artmadığını veya azalıp azalmadığını anlamak için kullanılır.
    - **İçerik:** Trend analizi raporları, özel tehdit türlerinin (örnek, phishing saldırıları, fidye yazılımı saldırıları) kişisel olarak sunulan sunumlar ve tablolarla sunulur.
    - **Kullanım:** Güvenlik ekipleri, artan tehdit türlerine karşı savunma stratejilerini ayarlamak için bu analizleri kullanır. Örneğin, belirli bir saldırı durumu ortaya çıkıyorsa, ilgili güvenlik önlemleri güçlendirilir.
- **Davranışsal Trendler:** Kullanıcı ve cihaz parametreleri analiz edilir ve normalden sapmalar tespit edilir. Bu, normal işlemlerin (örneğin, günün yüksek veri aktarımı, olağandışı kesintilerin giriş yapılmasını) daha iyi anlaşılmasını sağlar.
    - **İçerik:** Kullanıcının süresi, belirli dönemlerdeki anormal aktiviteler ve bunların sistem üzerindeki etkileri analiz edilir. Örneğin, belirli bir kullanıcı hesabı gece saatlerinde sürekli olarak giriş yapıyorsa, bu bir iç tehdit belirtisi olabilir.
    - **Kullanım:** Davranışsal trend analizleri, iç tehditleri ve kullanıcı hatalarını tespit etmek için kullanılır. Güvenlik politikaları, bu analizlere dayalı olarak güncellenir.
- **Risk Profili Geliştirme:** Trend analizleri, günün genel risk profilini geliştirme. Zamanın içindeki değişiklikler, riskin artıp artmadığını veya yeni tehditlerin ortaya çıkmadığını gösterir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **İçerik:** Risk profilinin yapısal özellikleri (birçok, saldırı türleri, hedeflenen varlıklar, saldırıların başarı oranı) detaylandırılır.
- **Kullanım:** Yönetim ve güvenlik stratejileri ekipleri, risk profilindeki değişikliklere dayalı olarak güvenlik bütçelerini, yatırımlarını ve parlaklıklarını belirler.

1.1.1.5.4 Yasal ve Uyumluluk Raporları

Bazı endüstri, belirli güvenlik düzenlemeleri ve yasal gerekliliklere uyum sağlanır. SIEM sistemlerinin, bu bölümlerinin sağlanması ve dağıtıcı raporlama yapmak için gerekli verilerin sağlanması sağlanır.

- **Uyumluluk Raporları:** SIEM sistemleri, PCI DSS, GDPR, HIPAA gibi düzenlemelere uyumu sağlamak için gerekli ayarlar oluşturulur.
  - **İçerik:** Uyumluluk raporları, kapsamlı standartların gerekliliklerine göre logların analizini, tehditlerin değerlendirilmesini ve alınan güvenlik önlemlerini içerir.
  - **Kullanım:** Bu raporlar, yasal denetimler sırasında yardımlaşmanın entegre gerekliliklere ne ölçüde uyduğunu kanıtlamak için kullanılır.
- **Denetim Raporları:** SIEM, iç ve dış denetim kapsamlı için kapsamlı raporlar sunar. Bu raporlar, sistemlerin nasıl izlendiğini, hangi olayların tespit edildiğini ve nasıl yorumlandığını gösterir.
  - **İçerik:** Denetim raporları, log yönetimi, olay oranları, izleme paketleri ve güvenlik kontrolleri hakkında ayrıntılı bilgiler sunar.
  - **Kullanım:** Denetim raporları, iç güvenlik değerlendirmeleri ve dış denetim standartları için kullanılır. Bu raporlar, güvenlik açıklarının belirlenmesi ve sunulan öneriler değerlendirilebilir.

1.2 Alarm ve Uyarı Sistemleri

- **Gerçek Zamanlı Uyarılar:** Algılama sistemlerinden gelen uyarılar, güvenlik operasyonu çalıştırma (SOC) veya belirli kişilere anında bildirilir. Bu bildirimler, e-posta, SMS, anlık mesajlaşma araçları veya sesli uyarılar şeklinde olabilir.
- **Alarm Eşik Değerleri:** Güvenlik sistemleri, belirli bir eşik değeri üzerinde alarm verdiğinde verir. Bu eşikler, sistem bağlantıları tarafından yapılandırılır ve olası bir yanlış alarmı (yanlış pozitif) en aza indirmek için optimize edilir.
- **Önceliklendirme:** Tespit edilen olayların önem derecesine göre görünürlüğü belirlenir. Kritik olaylardaki olaylar hemen üst yönetime veya olay müdahale ekibine iletilir.

1.1.2 Saldırı Algılama Sistemleri (IDS) ve Saldırı Önleme Sistemleri (IPS)

Saldırı Tespit Sistemleri (IDS) ve **Saldırı Önleme Sistemleri (IPS)** , siber güvenlikte kullanılan iki kritik teknoloji grubudur. Her iki sistem değleri ve sistemleri üzerindeki tehditleri tespit etmek için kullanılır; Ancak bu sistemlerin işleyişleri ve yoğunlukları değişir. Bu bölümde IDS ve IPS sonuçlarının nasıl olduğu, hangi yöntemlerin uygulandığı ve organizasyonların nasıl yapıldığı ayrıntılı olarak ele alındı.

1.1.2.1 Saldırı Algılama Sistemleri (IDS)

IDS, bir ağ veya sistem ortaya çıkan şüpheli veya kötü niyetli performansları izliyor ve raporlar. IDS'ler, genellikle pasif bir rol oynar ve tespit edilen saldırılar veya güvenlik ihlalleri hakkında uyarı verir. IDS sistemleri, saldırganların sistemlerine veya ağlara yetkisiz erişime sahip olup olmadığının belirlenmesi için kullanılır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1.1.2.1.1 Çeşitleri

- **Ağ Tabanlı IDS (NIDS):** Ağ tabanlı IDS, ağ akışını izlemeyi potansiyel tehditleri tespit eder. Bu tür sistemlerde, kritik noktalara yerleştirilir ve gelen ve giden tüm trafik paketlerini analiz eder.
    - **Örnek kullanım:** Bir NIDS, belirli bir ağ segmentindeki tüm şebekeyi dinleyerek, ağda anormal durumları (bunlar, şüpheli port taramaları, yüksek hacimli veri çıkışı) olup olmadığını kontrol eder.
    - **Avantajları:** NIDS, ağın genel içeriğini arttırır ve ağın tamamını kapsayabilir. Bu tür bir IDS, ağ tabanlı saldırılara (örneğin, DDoS, MITM saldırıları) karşı oldukça etkilidir.
- **Host Tabanlı IDS (HIDS):** Host tabanlı IDS, bireysel cihazlar (örneğin, sunucular, iş istasyonları) üzerinde çalışır ve bu cihazlarda alınır. HIDS, işletim sistemi logları, dosya bütünlüğü, kullanıcı faaliyetleri ve diğer sistem tabanlı analizler izlenir.
    - **Örnek Kullanım:** Bir HIDS, bir sunucudaki kritik dosyalara yapılan tüm erişimleri izleyebilir ve bu dosyalarda herhangi bir yetkiliz değişiklik gösterme izni verilebilir.
    - **Avantajları:** HIDS, belirli bir cihaz üzerinde çok daha ayrıntılı izleme yapar ve sistemin içindeki tehditleri tespit etme konusunda oldukça etkilidir.

1.1.2.1.2 Test Yöntemleri

- **İmza Tabanlı Tespit:** IDS sistemleri, bilinen saldırı kalıplarını veya imzalarını tespit etmek için imza tabanlı olarak bulunabilir. Bu yöntemde, IDS sistemi saldırılara özgü bilinen imzalarla gelen veriler karşılaştırılır.
    - **Örnek:** Bir IDS, belirli bir kötü amaçlı yazılımın kaydedilmesini imzalamak için kullanılabilir. Gelen veri aktarımında bu imzaya uygun bir şey tespit edilirse, IDS bir uyarı verir.
    - **Avantajları:** İmza tabanlı tespit, bilinen tehditlere karşı son derece etkili ve hızlıdır.
- **Anomali Tabanlı Tespit:** Anomali temelli tespit, normal sistemin oluşumuna karşı sapmaları tespit eder. Bu yöntem, sistem veya ağın normal öğrendiğini öğrenir ve bu duruma uymayan herhangi bir anormallik bir potansiyel tehdit olarak işaretler.
    - **Örnek:** genellikle belirli bir port üzerinden çok az trafik geçiren bir sunucuda, bu port üzerinden yoğun trafik yaşanan bir anormallik olarak bulunabilir.
    - **Avantajları:** Bu yöntem, bilinmeyen tehditleri tespit etmede ve sıfırıncı gün (sıfır gün) saldırılarına karşı etkili olabilir.
- **Hibrit Tespit:** IDS sistemleri, imza tabanlı ve anomalilerin ayrıntılarını birleştiren hibrit parçalar kullanılabilir. Bu sayede hem bilinen hem de bilinmeyen tehditlere karşı daha geniş kapsamlı bir koruma sağlandı.
    - **Örnek:** Bir IDS, hem bilinen saldırı imzalarını hem de anormal ağ değişimlerini izleyerek daha güvenilir bir tespit bölgeleri bölgeleri.
    - **Avantajlar:** Hibrit kırılmalar, tespit doğruluğunun artması ve yanlış pozitiflerin azalması.

1.1.2.1.3 IDS'in Sınırlamaları

- **Pasiflik:** IDS'ler genellikle sadece tespit ve uyarı verir, ancak saldırılara karşı doğrudan müdahalede bulunmazlar. Bu da, karşılanacak aksiyonların tamamen güvenlik ekiplerine aktarılmasını sağlar.
- **Yanlış Pozitifler (Yanlış Pozitifler):** İmza temelli tespit yöntemlerinde olabilir, yanlış pozitifler yaygın. Bu, normal gidişin yanlışlıkla tehdit olarak algılanması durumudur ve güvenlik ekiplerinin gereksiz yere uyarlanmasına yol açabilir.
- **Bilinen İmzalara Bağımlılık:** İmza tabanlı IDS'ler, yalnızca daha önceden tanımlanmış tehditleri tespit edebilir. Yeni veya tanımlanmamış tehditler, bu tür sistemler tarafından kaçırılabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1.1.2.2 Saldırı Önleme Sistemleri (IPS)

IPS, IDS sistemlerine benzer şekilde çalışır ancak tespit ettiği tehditlere karşı aktif olarak müdahale eder. IPS, bir ağ veya sistemdeki potansiyel tehditleri önlemek için tasarlanmıştır. IPS, bir IDS'nin tüm yeteneğinin özellikleri yanı sıra, tehditlerin engellenmesi ve saldırıları için ek özellikler içerir.

1.1.2.2.1 Çalışma Prensibi

IPS sistemlerini, ağ bağlantılarını ve sistem aktivitelerini sürekli olarak potansiyel izleme tehditlerini belirler ve bunları karşıdan takip edersiniz. IPS, bir ağda gerçekleşen tüm verileri inceler ve zararlı olduğu tespit edilen aktarımları engelleyebilir, yönlendirebilir veya düşürebilir.

- **Ağ Trafiği İzleme:** IPS, ağa gelen ve giden tüm trafiğe ait gerçek zamanlı olarak izler. Bu trafik, belirli kurallar ve politikalar analiz edilir. Örneğin, belirli portlardan gelen olağan dışı veri değişimleri, güvenlik açıklarından yararlanmaya çalışan saldırılar veya bilinen zararlı yazılım imzalarını içeren trafik gibi durumlar tespit edilir.
- **Paket Analizi:** IPS, ağ üzerindeki bir veri paketini analiz eder. Bu analiz, paketlerin verileri, kaynak ve hedef IP adreslerini, kullanılan protokolleri ve diğer meta verileri içerir. Zararlı olarak tanımlanmış paketler anında engellenir.
- **Durum Tabanlı İnceleme:** IPS, bağlantıların izlediği ayrı bir giriş veya bağlantıdaki anormallikleri tespit eder. Bu sayede, yalnızca tekil paketler değil, aynı zamanda tümlerin iletiminin genel performansı da incelenir.

1.1.2.2.2 Tespit ve Müdahale Yöntemleri

IPS sistemleri, tehditleri tespit etmek ve bunlara karşı otomatik olarak müdahale etmek için çeşitli kullanılabilir. Bu kırılmalar, tehdit türlerine ve bireylerin güvenliğine göre değişiklik yapılabilir.

1.1.2.2.2.1 İmza Tabanlı Müdahale

İmza tabanlı IPS, bilinen tehditlerin belirli kalıplarını (imzalarını) tespit etmek için kullanılır. Bu imzalar, daha önceden tanımlanmış zararlı özelliklerin özelliklerini içerir ve IPS bu imzaları kullanımda otomatik olarak müdahale eder.

- **Çalışma Prensibi:** İmza tabanlı IPS, veri tabanında bulunan zararlı imzalarla ağ aktarımını karşılaştırır. Bu imzalar, belirli saldırı türlerinin (örneğin, SQL dosyaları, DDoS saldırıları) bilinen örneklerini içerir.
    - **Örnek:** Eğer bir IPS, bir SQL saldırı saldırısına özgü bir dizi karakter dizisini tespit ederse, bu bozulmaları engeller ve saldırıyı durdurur.
- **Avantajları:** İmza temelli tespit hızlıdır ve bilinen tehditlere karşı son derece etkilidir. Bilinen saldırı türlerine karşı güvenilir bir koruma sağlar.
- **Sınırlamalar:** İmza tabanlı IPS sistemleri, yalnızca veri tabanında bulunan imzalara dayalı olarak tehditleri tespit edebilir. Bu nedenle, sıfırıncı gün (sıfır gün) saldırılarını veya bilinmeyen tehditleri tespit etme konusunda yetersiz olabilir.

1.1.2.2.2.2 Anomali Tabanlı Müdahale

Anomali tabanlı IPS, ağ dağıtımı veya sistem performansındaki olağandışı durumları tespit etmek için kullanılır. Bu yöntem, belirli bir sistem veya ağın normal öğrendiğini öğrenir ve bu davranıştan sapmaları potansiyel tehdit olarak değerlendirir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Çalışma Prensipleri:** Anomali tabanlı IPS, bir sistem veya ağın normal çalışma analizini yapar ve bunları bir temel çizgi (baseline) olarak kabul eder. Bu çizgiden sapmalar, potansiyel bir tehdit olarak algılanır ve bu şekilde müdahale edilir.
    - **Örnek:** genellikle küçük dosya aktarımları gerçekleştiren bir sunucunun, büyük miktarda veri göndermeye başladığı durumda, anormal temelde bir IPS bu durumu şüpheli bulur ve veri aktarımı engellenebilir.
- **Avantajları:** Anomali tabanlı tespit, bilinmeyen veya yeni tehditlerin tespitinde etkili. Bu yöntem, sıfırıncı gün saldırıları gibi henüz tanımlanmamış tehditlere karşı koruma sağlar.
- **Sınırlamalar:** Anomali temelli tespit, yanlış pozitiflerin (yanlış pozitifler) çoğaltılabilir. Normal olmayan ancak zararsız faaliyetler, tehdit olarak algılanabilir ve gereksiz müdahalelere neden olabilir.

1.1.2.2.2.3 Durum Tabanlı Müdahale (Durum Denetimi)

Durum tabanlı IPS, ağ dağıtımını sadece tekil paketler bazında değil, aynı zamanda bu paketlerin kayıtlı kayıtları inceler. Bu yaklaşım, paketlerin belirli bir sıra ve bağlama içerisinde değerlendirilmesini sağlar.

- **Çalışma Prensipleri:** Durum tabanlı IPS, bir anahtarın veya işletmenin kontrolünün bitişine kadar geçen süreyi izler ve bu süre zarfındaki sıcaklık rejimini analiz eder. Bu şekilde normalden sapmalar gösteren yapılar tespit edilir.
    - **Örnek:** Normalde birkaç tane tamamlanan bir kişinin, kendisinden çok daha uzun sürmesi veya çok fazla veri taşıması, durumsal bir anormallik olarak işlenmesi.
- **Avantajları:** Bu yöntem, uzun süreli ve çok dağınık saldırıların tespit edilmesinde etkilidir. Örneğin, bir Salgının birden fazla oturumda birden fazla koruma sisteminin ele geçirmeye çalışması durumunda, bu saldırı durumsal olarak tespit edilebilir.
- **Sınırlamalar:** Durum temelli tespit, daha karmaşık birimler gerektirir ve bu nedenle diğer hızlarla karşılaştırma daha yüksek işlem gücü ve gecikme süresi gerektirir.

1.1.2.2.3 IPS'in Avantajları ve Sınırlamaları

IPS verimi verimliliği, doğruluğu ve uygun kullanım koşulları bağlıdır. IPS, ağ harcamalarının proaktif bir şekilde yönetilmesine olanak tanır, ancak sistemin etkili olması için bazı avantaj ve sınırlamalar göz önünde bulundurulmalıdır.

1.1.2.2.3.1 Avantajlar

- **Aktif Koruma:** IPS sistemleri, tespit tehditlerine karşı anında müdahale eder. Bu, saldırıların gerçekleşmesinden önce durdurulmasını sağlar.
- **Gerçek Zamanlı Yanıt:** IPS, tehditlerin tespit edildiği anda müdahale edilebilir, bu da saldırıların zararının azaltılmasından önce engellenmesini sağlar. Özellikle hızlı hareket eden tehditler (örneğin, DDoS saldırıları) için bu son derece kritiktir.
- **Gelişmiş Güvenlik:** IPS sistemleri, ağ bağlantılarını ve sistem aktivitelerini sürekli olarak izleme, bilinmeyen tehditleri tespit etme yeteneğine sahiptir. Anormal kalınlıklarda, yeni tehditlere karşı koruma sağlar.
- **Otomatik Müdahale:** IPS, güvenlik ekiplerinin müdahalesine gerek kalmadan tehdit tehditlerini otomatik olarak engelleyebilir. Bu, insan hatalarını azaltır ve tehditlerin hızla durdurulmasını sağlar.

1.1.2.2.3.2 Sınırlamalar

- **Yanlış Pozitifler (Yanlış Pozitifler):** Anomali tabanlı IPS sistemlerinde, yanlış pozitiflerin miktarı yüksek olabilir. Bu, normal eylemlerin yanlışlıkla tehdit olarak algılama anlamına gelir ve gereksiz müdahalelere yol açabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **İşlem Gücü Gereksinimleri:** IPS sistemleri, ağ kesintisini gerçek zamanlı olarak analiz etmek ve müdahale etmek için önemli miktarda işlem gücü ve kaynak gerektirir. Bu, özellikle büyük ayarlar için bir performans sorunu çözer.
- **Kompleks Kurulum ve Yönetim:** IPS yazılımının doğru yapılandırılması ve birim karmaşık olabilir. Yanlış kurulum, sistemin düşmesine neden olabilir veya tehditlerin kaçırılmasına neden olabilir.
- **Bilinen Tehditlere Bağımlılık:** İmza taban

1.1.2.2.2 Tespit ve Müdahale Yöntemleri

- **İmza Tabanlı Müdahale:** IPS,şu anda IDS gibi imza tabanlı olarak konumlandırılabilir. Ancak tespit edilen tehditlere karşı aktif müdahalede bulunuluyor.
    - **Örnek:** Bilinen bir zararlı yazılım imzasının tespit edilmesi, IPS bu yazılımın içine giriş yapılmasını engeller.
    - **Avantajları:** Bilinen tehditlere karşı hızlı ve etkili müdahale sağlar.
- **Davranış Tabanlı Müdahale:** IPS, ağ şebekelerini ve sistem değişikliklerini analiz ederek anormallikleri tespit eder ve bu anormalliklere karşı müdahale eder.
    - **Örnek:** Genellikle küçük veri transferleri yapan bir cihazın büyük miktarda veri göndermeye başlaması durumunda, IPS bu arızaları durdurabilir ve daha fazla analiz için güvenlik ekibine bildirebilir.
    - **Avantajları:** Yeni veya bilinmeyen tehditleri tespit etmede ve önlemede etkili olabilir.

1.1.2.2.3 IPS'in Avantajları ve Sınırlamaları

- **Avantajlar:**
    - **Aktif Koruma:** IPS, tespit edilen tehditlere karşı anında müdahale ederek saldırıları durdurur. Bu, ağ maliyetlerini proaktif olarak yönetmeyi sağlar.
    - **Gerçek Zamanlı Yanıt:** IPS sistemlerinde, tehditlerin tespit edildiği anda müdahale edilebilir, bu da saldırıların zararının durdurulmadan önce durdurulmasını sağlar.
    - **

1.1.3 Anormal *Algılama* Sistemleri

Anomali Algılama Sistemleri , bir ağ veya sistemin normal işleyişinden sapmaları tespit etmek için kullanılır. Bu sistemler, özellikle bilinmeyen tehditleri ve sıfırıncı gün saldırılarını belirlemede etkilidir. Anormal algılama, sistem veya alışılmış öğrenilenler öğrenir ve bu normal davranıştan sapmaları potansiyel tehdit olarak değerlendirilir.

1.1.3.1 Çalışma Prensibi

Anormallik algılama sistemleri, belirli bir zaman diliminde sistem veya ağın normal olarak öğrendiği ve bu bilgiyi temel çizgi (baseline) olarak kullanır. Bu temel çizgiye dayalı olarak, normalden sapmayı gösteren herhangi bir davranış veya etkinlik, anormallik olarak işaretlenir.

- **Temel Çizgi Oluşturma:** Anomali algılama sistemleri, ağ kabloları, sistem özellikleri, kullanıcı gelişimi gibi veriler toplar ve bunları analiz ederek bir temel çizgi oluşturur. Bu temel çizgi, sistemin normalliğini temsil eder.
    - **Örnek:** Bir sunucunun normal günün içindeki veri çıkışı belirli bir aralıkta olabilir. Eğer bu sunucudan çok daha fazla veri çıkışı olursa, bu durum bir anormallik olarak işaretlenebilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Sapma Tespiti:** Anomali algılaması, sürekli olarak ağ bağlantılarını ve sistem aktivitelerini izliyoruz. Bu izleme sırasında, temel çizgiden sapmalar farklılıkları, sistem bu durumu olası bir tehdit olarak değerlendirilir.
    - **Örnek:** Bir kullanıcı normalde çalışma ayarları sisteme giriş yaparken, gece boyunca aynı kullanıcıdan anında fazla giriş denemesi yapılırsa, bu durum bir anormallik olarak tespit edilebilir.

1.1.3.2 Anormal Algılama Yöntemleri

Anormal algılama sistemleri, çeşitli büyüklükleri kullanarak normalden sapmaları tespit eder. Bu dönüşümler, sistemin karmaşıklığına ve izlenen ortamın karmaşıklığına göre değişir.

1.1.3.2.1 İstatistiksel Yöntemler

İstatistiksel ölçümler, sistem veya ağ sonuçlarının ortalama değerleri, varyanslarını ve diğer ölçümleri hesapları. Bu ölçümler temel alınarak anormal durumlar tespit edilir.

- **Çalışma Prensipleri:** İstatistiksel anormallik algılaması, belirli bir zaman dilimindeki verilerin ortalamasını ve gidişatını belirler. Bu normal dağılımdan sapmalar, anormallik olarak kullanılır.
    - **Örnek:** Bir web sunucusuna yapılan sayı günlük olarak belirli bir ortalama değer etrafında yoğunlaşır. Eğer belirginliğin devamı büyük bir artış olursa, bu durum bir anomali olarak tespit edilebilir.
- **Avantajlar:** İstatistiksel ilerleme basit ve hızlıdır. Geniş veri kümeleri üzerinde çalışır ve genellikle iyi sonuçlar verir.
- **Sınırlamalar:** İstatistiksel parçacıklar, karmaşık veya çok sayıda saldırıların tespit edilmesinde yetersiz olabilir. Ayrıca, çok sayıda yanlış pozitif üretme potansiyeline sahiptir.

1.1.3.2.2 Makine Öğrenmesi Tabanlı Yöntemler

Makine öğrenmesi yapısal anormallik algılaması, sistemin normal davranışları arasındaki farklar için kullanır ve bu öğrenilen davranışlarından sapmaları tespit eder.

- **Çalışma Prensipleri:** Makine öğrenmesi gelişmeleri, sistemin normal gidişatı için büyük miktarda veriyi analiz eder. Bu öğrenme sürecinin ardından sistem yeni verileri bu normal davranışlarla karşılaştırılır ve hatalar tespit edilir.
    - **Örnek:** Bir kullanıcı davranış modeli oluşturulabilir. Kullanıcıların tipik işlem modelleri (örneğin, hangi dosyalara eriştikleri, hangilerinin çalıştıkları) öğrenilir ve bu modelden sapmalar anormal olarak kullanılır.
- **Avantajları:** Makine öğrenmesi tabanlı çözümler, dinamik ve karmaşık ortamda yüksek doğrulukla çalışır. Bilinmeyen tehditleri ve sıfırıncı gün saldırılarını tespit etmede etkilidir.
- **Sınırlamalar:** Bu iyileştirmeler, eğitim süresi ve işlem gücü gerektirir. Ayrıca, büyük veri kümeleri gerektirir ve yanlış pozitiflerin sayısını azaltmak için sürekli olarak optimize edilmelidir.

1.1.3.2.3 Zaman Serisi Analizi

Zaman serisi analizi, sistem veya ağ üzerindeki olayları zaman İç düzenini inceleyerek, belirli bir zaman diliminde ortaya çıkan anormallikleri tespit eder.

- **Çalışma Prensipleri:** Zaman serisi analizi, belirli bir olayın zaman içindeki desenini analiz eder ve bu desenin normalden sapmalarını tespit eder.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Bir sunucunun CPU çalışmasının gün boyunca düzenli olarak belirli bir desen izlemesi yapılıyor. Bu desenin içerdiği ani bir artış veya azalma olursa, bu bir anormallik olarak değerlendirilebilir.

- **Avantajları:** Zaman serisi analizi, belirli zaman dilimlerinde ortaya çıkan, gelen olağandışı olayları tespit etmekte etkili bir yöntemdir. Özellikle aralıklı tekrarlayan saldırıların belirlenmesi için kullanışlıdır.
- **Sınırlamalar:** Zaman serisi analizi, zamana dayalı olmayan anormalliklerin tespitide yetersiz olabilir. Ayrıca, çok fazla veri noktası içeren karmaşık zaman serileri için analiz süresi uzun olabilir.

1.1.3.3 Anormal Algılama Sistemlerinin Avantajları ve Sınırlamaları

Anormal algılama sistemleri, özellikle bilinmeyen veya yeni ortaya çıkan tehditleri tespit etmek için etkili bir araçtır. Ancak bu sistemlerin bazı zaman aralıkları ve sınırlamaları vardır.

1.1.3.3.1 Avantajlar

- **Bilinmeyen Tehditlerin Tespiti:** Anomali algılama sistemleri, sıfırıncı gün saldırıları veya henüz tanınmamış tehditler gibi bilinmeyen saldırıları tespit edilebilir.
- **Dinamik Öğrenme Yeteneği:** Makine öğrenmesi temelli anormallik algılama sistemleri, sürekli olarak güncellenen tehdit ortamına uyum sağlayabilir ve yeni tehditleri tespit etmede etkili olabilir.
- **Geniş Kapsam:** Anomali algılama, ağ dağılımı, sistem işleyişi, kullanıcı faaliyetleri ve diğer birçok veri özelliklerini kapsayabilir. Bu da çok yönlü bir güvenlik koruması sağlar.

1.1.3.3.2 Sınırlamalar

- **Yanlış Pozitifler:** Anormal algılama sistemleri, normalden sapmaları potansiyel tehdit olarak değerlendirdiği için, yanlış pozitiflerin sayıları yüksek olabilir. Bu, güvenlik sistemlerinin gereksiz yere uyarlanmasına yol açabilir.
- **Yüksek Hesaplama Maliyetleri:** Özellikle makine öğrenmesi tabanlı sistemler, büyük veri kitapları üzerinde çalışan yüksek programlama gücü gerektirir. Bu da masrafları azaltabilir ve performans sorunlarına yol açabilir.
- **Kompleks Yapılandırma:** Anomali algılama sonuçlarının doğru şekilde yapılandırılması ve optimize edilmesi karmaşık bir şekilde sağlanır. Yanlış yazılımlar, sistem bozuklukları düşürebilir veya tehditleri kaçırmasına neden olabilir.

1.1.4 Log Yönetimi

Log Yönetimi, siber güvenlikte kritik bir unsurdur. Bir organizasyonun ağında veya sistemlerinde gerçekleşen tüm etkinliklerin kaydedilmesi, bu etkinliklerin analiz edilmesi ve yasal düzenlemelere uygun olarak raporlanması önemlidir. Loglar, bir güvenlik olayı meydana geldiğinde olaya dair izlerin sürülmesini ve bu olayın kökeninin anlaşılmasını sağlar. Log yönetiminin doğru bir şekilde uygulanması, hem saldırıların tespiti hem de olay sonrası analizlerin yapılabilmesi açısından hayati önem taşır.

1.1.4.1 Log Toplama

- Log toplama, log yönetiminin ilk adımıdır ve çeşitli kaynaklardan alınan log verilerinin merkezi bir yerde toplanmasını içerir. Bu loglar, genellikle ağ cihazları, sunucular, güvenlik duvarları, işletim sistemleri, uygulamalar ve diğer güvenlik araçlarından elde edilir.
- Formül 1: Toplam Log Miktarı (TLM) Hesabı:
- TLM = Σ Li, i=1 to N
  TLM toplam log miktarını ifade eder, Li her bir kaynaktan gelen log miktarını gösterir, N ise log kaynaklarının toplam sayısını temsil eder.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1.1.4.2 Log Depolama ve Yönetim

- Toplanan loglar, merkezi bir log yönetim sisteminde depolanır. Logların güvenli bir şekilde saklanması ve gerektiğinde kolayca erişilebilmesi için doğru bir şekilde organize edilmesi önemlidir.
- Formül 2: Log Normalleştirme Süresi (LNS) Hesabı:
- LNS = Σ (Si / Ri), i=1 to N
  LNS log normalizasyon süresini ifade eder, Si her kaynaktan gelen log miktarını, Ri ise kaynağın normalizasyon hızını (MB/saniye) gösterir.

1.1.4.3 Log Analizi ve İzleme

- Logların analizi, güvenlik tehditlerinin tespit edilmesi ve olaya müdahale için kritik bir adımdır. SIEM gibi araçlar, logların analizini otomatikleştirir ve güvenlik olaylarını tespit eder.
- Formül 4: Korelasyon Sayısı (KS) Hesabı:
- KS = Σ Ci, i=1 to N
  KS toplam korelasyon sayısını, Ci her bir log kaynağının belirlediği korelasyon miktarını gösterir.

1.1.4.4 Log Raporlama

- Log verilerinden elde edilen bulgular düzenli olarak raporlanır. Bu raporlar, hem teknik ekipler hem de yöneticiler için kritik bilgiler sunar.
- Formül 5: Raporlama Sıklığı (RS) Hesabı:
- RS = TLM / P
  RS raporlama sıklığını, TLM toplam log miktarını ve P raporlanacak dönemi ifade eder.

1.1.4.5 Log Yönetiminin Avantajları ve Sınırlamaları
1.1.4.5.1 Log Yönetiminin Avantajları

Log yönetimi, siber güvenlik sistemlerinin gelişiminin artırılması ve bir organizasyonun bilgi teknolojilerinin sunumunun sağlanması için kritik bir sağlanır.

1. Güvenlik İyileştirmeleri:

- **Tehdit Tespiti:** Loglar, sistem
- **Olay Müdahalesi:** Bir saldırının içeriğinde veya sistemin bir güvenlik merkezindeki yerleşimi

2. Olay Sonrası Analiz:

- **Adli Bilişim:** Loglar
- **Sorun Giderme:** Bir sorun

3. Yasal Uyumluluk:

- **Yasal Gerekliliklerin Karşılanması:** Bir çok gelişmiş, yasal düzenlemelerin yapılması belirli sürelerle logların saklanması zorunludur. Örneğin sağlık ve finans sektörlerinde müşteri bilgileri ve işlem kayıtlarının loglanması ve saklanması gerekmektedir. Kayıt
- **Denetim Raporu:** Denetim sırasında loglar, organizasyon

4. Performans İzleme ve İyileştirme:

- **Sistem Performans İzleme:** Log

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Proaktif Bakım:** Log verileri sistemi sayesinde oluşabilecek olası arızalar veya yavaşlamalar önceden tespit edilebilir. Bu da proaktif

5. Otomatikleştirilmiş Güvenlik Analizleri:

- **SIEM Entegrasyonu:** Log yönetimi sistemleri genel
- **Korelasyon ve Anomali Tespiti:** Farklı kaynaklardan gelen loglar analiz edilerek anormal davranışlar tespit edilebilir. Bu da karmaşık saldırıların veya iç tehditlerin belirlenmesine olanak sağlar.

1.1.4.5.2 Log Yönetimi Sınırlamaları

Log yönetimi, bir organizasyonun güvenliğinin kaydedilmesi ve analiz edilmesi açısından büyük avantajlar sunsa da, bazı sınırlamalar da beraberinde gelir. Bu sınırlamalar, hem tek

1. Depolama Maliyetleri:

- **Büyük Veri Miktarı:** Büyük şık organizasyon
- **Uzun Süreli Saklama Gereksinimi:** Yasal düzenlemeleri

2. Yüksek Analiz Süresi:

- **Veri Yoğunluğu:** Büyük veri hacimlerinin analizi, özellikle
- **Yavaş İşlem:** Logların ko

3. Gizlilik Riskleri:

- **Log Verilerinin Güvenliği:** Log dosyalarındaki kullanıcı işlemleri, IP adresleri, sistem analizleri gibi hassas bilgiler bulunabilir. Bu kişilerin yetkisiz erişimlerinin korunması, ek güvenlik harcamaları gerektirir. Eğer loglar şifrelenmeden veya güvenlik önlemleri alınmadan saklansa, bu durum ciddi Gizlilik ve güvenlik risklerine yol açabilir.
- **İç Tehditler:** Log veri

4.Yanlış Alarm (Yanlış Pozitif) Riski:

- **Yanlış Uyarılar:** Log yönetim sistemleri, b
- **Alarm Yorgunluğu:** Sürekli gelen yanlış uyarılar, güvenlik ekiplerinde “alarm yorgunluğunu” yaratabilir. Bu da gerçek tehdit

5. İş Gücü ve Kaynak Gereksinimi:

- **Uzmanlık Gerektiren Bir Süreç:** Log yönetimi, hem teknik bilgi hem de den
- **Otomasyon İhtiyacı:** Manuel log analizi ve yönetimi zaman alıcı ve

6. Uyumluluk ve Entegrasyon Zorlukları:

- **Farklı Sistemlerle Entegrasyon:** Bir organizasyonda kullanılan farklı sistemler ve cihazlar, farklı log formatlarına ve yapılarına sahip olabilir. Tüm bu kayıtlı tek bir sistemi içerir, normalleştirme ve analiz etme güçlüğünü gerçekleştirebilirsiniz. Logların ortak bir formata dönüştürülmesi zaman alıcı olabilir.
- **Yazılım Uyumluluğu:** Log yönetimi

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1.3 Olayın Bildirilmesi

1.3.1 Olayın Tanımlanması

- Olayın doğru şekilde tanımlanması, sürecin ilk adımıdır. Olayın türü, etkilediği sistemler ve potansiyel zarar belirlenir.
- Formül: OT = ET + ES
- Açıklama: OT: Olayın Tanımı, ET: Etkilenen Teknolojiler, ES: Etkilenen Sistemler

1.3.2 Bildirim Seviyesi

- Olayın aciliyeti ve kapsamı, hangi seviyede bildirim yapılacağını belirler.
- Formül: BS = SE + CE
- Açıklama: BS: Bildirim Seviyesi, SE: Sistemin Etkilenme Seviyesi, CE: Kullanıcılara Etki Seviyesi

1.3.3 Bildirilecek Tarafların Belirlenmesi

- Farklı olaylar farklı taraflara bildirilmelidir. Olayın büyüklüğüne göre bildirilecek taraflar belirlenir.
- Formül: BT = EC + YO + D
- Açıklama: BT: Bildirilecek Taraflar, EC: Etkilenen Çalışanlar, YO: Yasal Otoriteler, D: Departmanlar

1.3.4 Bildirim Süresi

- Olayın ne kadar sürede bildirileceği, yasal ve iç süreçlere bağlıdır.
- Formül: BSU = OTS + RT
- Açıklama: BSU: Bildirim Süresi, OTS: Olay Tespit Süresi, RT: Yanıt Zamanı

1.3.5 Olayın Ciddiyet Seviyesi

- Olayın ciddiyet seviyesi, müdahale önceliğini belirler.
- Formül: CS = IS + DS
- Açıklama: CS: Ciddiyet Seviyesi, IS: İşlemci (Sistem) Üzerindeki Etki, DS: Zarar Seviyesi

1.3.6 Olayın Etki Alanı

- Olayın etki alanı, olayın etkilediği kullanıcı sayısı ve sistemlerle belirlenir.
- Formül: EA = KU x ES
- Açıklama: EA: Etki Alanı, KU: Etkilenen Kullanıcı Sayısı, ES: Etkilenen Sistemler

1.3.7 Bildirimin Formatı

- Olay bildirimleri yazılı veya telefon gibi farklı formatlarda yapılabilir.
- Formül: BF = IF + WF
- Açıklama: BF: Bildirim Formatı, IF: İlk Bildirim Formatı, WF: Yazılı Bildirim Formatı

1.3.8 Bildirim İçeriği

- Bildirimin içeriğinde olay detayları, zarar raporu ve müdahale yöntemleri yer almalıdır.
- Formül: BI = OD + ZR + OM
- Açıklama: BI: Bildirim İçeriği, OD: Olay Detayları, ZR: Zarar Raporu, OM: Müdahale Yöntemleri

1.3.9 Yasal Bildirim Gereksinimleri

- Yasal düzenlemelere uygun olarak olaylar raporlanmalıdır.
- Formül: YB = OR + YG
- Açıklama: YB: Yasal Bildirim, OR: Olayın Rapora Dönüştürülmesi, YG: Yasal Gereklilikler

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- ### *1.3.10 Takip ve İzleme Süreci*
- Olayın bildirimi sonrası etkiler takip edilmeli ve süreç izlenmelidir.
- Formül: TI = FO + TO
- Açıklama: TI: Takip ve İzleme, FO: İlk Olay Sonrası İzleme, TO: Tamamlanma Oranı

- ### *1.3.11 İyileştirme ve Geri Bildirim*
- Olay sonrasında geri bildirim alınmalı ve sistem iyileştirmeleri yapılmalıdır.
- Formül: IG = SO + YO
- Açıklama: IG: İyileştirme Gereksinimleri, SO: Sistemdeki Olası Güvenlik Açıkları, YO: Yasal Otoritelerden Gelen Geri Bildirim
- **Otomatik Bildirim:** SIEM veya diğer izleme sistemleri, kaydedilen olaylar için otomatik olarak olay müdahale ekibine bildirim gönderilir. Bu bildirimler, olayların oluşumları ve potansiyel etkileri hakkında bilgi içerir.
- **Kullanıcı Bildirimi:** Kullanıcılar, şüpheli faaliyetlerin farklarındaki güvenlik ekiplerine manuel olarak bildirimde bulunabilirler. Bu tür bildirimler genellikle içe yönelik kimlik avı saldırıları, şüpheli e-posta veya yetkiliz erişim denemeleri gibi yaşanabilir.
- **Bildirim unsurları:** Organizasyon içinde, kimin, nasıl ve ne zaman bir olayın bildirileceği net bir şekilde geliştirilmelidir. Bu prosedürler, olayın hızlı bir şekilde ele alınmasını sağlar.

1.4 Olay Kaydı ve Dokümantasyon

1.4.1 Olayın Kayıt Edilmesi
Olayın gerçekleştiği tarih ve saat, olayın türü ve etkilediği sistemler dokümante edilmelidir.
Formül: OK = OT + TS + OID
Açıklama: OT: Olay Türü, TS: Tarih/Saat, OID: Olayın ID Numarası
Örnek: Örnek: OK = Kimlik Doğrulama Hatası + 2024-01-15 14:32 + 00123

1.4.2 Olayın Etkilenen Sistemleri
Olayın hangi sistemleri etkilediği ve hasar seviyesi dokümante edilmelidir.
Formül: ES = IS + HS
Açıklama: IS: İlgili Sistemler, HS: Hasar Seviyesi
Örnek: Örnek: ES = Web Sunucusu + Yüksek

1.4.3 Müdahale Ekiplerinin Kayıt Altına Alınması
Olaylara müdahale eden ekipler, rolleri ve hangi aşamalarda yer aldıkları kayıt altına alınmalıdır.
Formül: ME = TE + RE
Açıklama: TE: Teknik Ekip, RE: Roller ve Görevler
Örnek: Örnek: ME = Teknik Ekip + Güvenlik Uzmanları

1.4.4 Olayın Süresi
Olayın başlama ve bitiş zamanı dikkate alınarak olay süresi hesaplanmalıdır.
Formül: OS = OB - OT
Açıklama: OB: Olay Bitiş Zamanı, OT: Olay Başlama Zamanı
Örnek: Örnek: OS = 16:00 - 14:00 = 2 saat

1.4.5 Olayın Ciddiyet Seviyesi
Olayın sistemler üzerindeki etkisi ve iş sürekliliğine olan etkisi dokümante edilmelidir.
Formül: CS = IS + EO

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

Açıklama: IS: İlgili Sistemlerdeki Etki, EO: Etki Oranı
Örnek: Örnek: CS = Veritabanı + Yüksek Etki

1.4.6 Kayıt Sisteminin Tutulması

Olayın hangi sistemde kayıt altına alındığı dokümante edilmelidir.
Formül: KS = LS + MS
Açıklama: LS: Log Sistemi, MS: Müdahale Sistemi
Örnek: Örnek: KS = Log Yönetimi + SIEM

1.4.7 Hasarın Belirlenmesi

Olayın ardından ortaya çıkan zararın mali ve operasyonel boyutları hesaplanmalıdır.
Formül: HB = MO + TO
Açıklama: MO: Maddi Hasar, TO: Toplam Operasyonel Kayıp
Örnek: Örnek: HB = 10.000 + 3 saat

1.4.8 Bildirimlerin Kaydedilmesi

Olay hakkında yapılan tüm bildirimler, ilgili taraflar ve alınan aksiyonlar kaydedilmelidir.
Formül: BK = OID + BT
Açıklama: OID: Olay ID Numarası, BT: Bildirim Tarafları
Örnek: Örnek: BK = 00123 + Güvenlik Ekibi

1.4.9 Olay Sonrası Geri Bildirim

Olay sonrası yapılan geri bildirimler ve iyileştirme stratejileri kayıt altına alınmalıdır.
Formül: OGB = IS + GY
Açıklama: IS: İyileştirme Stratejileri, GY: Geri Bildirim Yöntemleri
Örnek: Örnek: OGB = İyileştirme + Raporlama

1.4.10 Yasal Gereksinimlerin Kayıt Edilmesi

Yasal gereksinimlerin karşılandığı ve ilgili kurumlara yapılan raporlamalar dokümante edilmelidir.
Formül: YGK = YB + SR
Açıklama: YB: Yapılan Bildirim, SR: Sunulan Raporlar
Örnek: Örnek: YGK = KVKK Bildirimi + Detaylı Rapor

1.4.11 Sistemlerin İyileştirilmesi

Olay sonrası yapılan iyileştirme çalışmaları ve sistemdeki değişiklikler kaydedilmelidir.
Formül: SI = SO + IG
Açıklama: SO: Sistem Özellikleri, IG: İyileştirme Gereksinimleri
Örnek: Örnek: SI = Veritabanı Güvenliği + Güvenlik Duvarı

1.4.12 Olayın Tekrarlanma Olasılığı

Benzer olayların tekrarlanma olasılığı, risk analizi ile hesaplanmalıdır.
Formül: TO = P × S
Açıklama: P: Olayın Tekrarlanma Potansiyeli, S: Sistem Zayıflığı
Örnek: Örnek: TO = 0.3 × 0.5

1.4.13 Olayın İzlenmesi

Olayın çözülme sürecinde yapılan tüm izleme faaliyetleri kaydedilmelidir.
Formül: OI = ST + IO
Açıklama: ST: Sistem Takibi, IO: İzleme Ortamı
Örnek: Örnek: OI = Sunucu İzleme + Ağ İzleme

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1.4.14 Olay Sonrası Raporlama

Olay sonrasında yapılan tüm raporlamalar kaydedilmeli ve taraflara sunulmalıdır.
Formül: OR = OID + IR
Açıklama: OID: Olay ID Numarası, IR: İç Raporlama
Örnek: Örnek: OR = 00123 + İç Rapor

1.4.15 Olayın Çözüm Süresi

Olayın çözüme ulaştırıldığı süre hesaplanmalı ve kayıt altına alınmalıdır.
Formül: OC = CE - CS
Açıklama: CE: Çözüm Bitiş Zamanı, CS: Çözüm Başlama Zamanı
Örnek: Örnek: OC = 10:00 - 1.5 Olayın Ön Değerlendirilmesi

- **Olayın Gerçekliği:** Bildirilen olayın gerçek olup olmadığının değerlendirilmesi gerekir. Yanlış alarmlar veya düşük hücresel olaylar, en verimli kullanım açısından filtrelenir.
- **Potansiyel Etki Analizi:** Sistemlerin çalıştırılması, yürütülmesi veya operasyonlara olası etkisi hızlı bir şekilde ulaştırılır. Bu, sürecin ne kadar acil olduğunun belirlenmesi için kullanılır.

1.5 Olay Müdahale Süreci

1.5.1 Olay Tespiti

- Olayın tespit edilmesi, müdahale sürecinin başlangıç noktasıdır. Bu aşamada güvenlik izleme sistemlerinden gelen alarmlar değerlendirilir.
- Formül: OT = LS + IS
- Açıklama: LS: Log Sistemi, IS: İzleme Sistemi
- Örnek: Örnek: OT = SIEM + İzleme Sistemi

1.5.2 Olay Doğrulaması

- Olayın gerçek bir tehdit olup olmadığının doğrulanması gerekir. Yanlış alarmlar veya güvenlik hatalarının önüne geçmek için olay doğrulaması yapılır.
- Formül: OD = OT + AI
- Açıklama: OT: Olay Tespiti, AI: Analitik İnceleme
- Örnek: Örnek: OD = Tespit Edilen Olay + Analitik İnceleme

1.5.3 Olayın Sınıflandırılması

- Olay, tehdit türüne ve ciddiyetine göre sınıflandırılır. Olayın türü, saldırının doğasına göre belirlenir (örneğin DDoS, fidye yazılımı, veri sızıntısı).
- Formül: OS = TT + CS
- Açıklama: TT: Tehdit Türü, CS: Ciddiyet Seviyesi
- Örnek: Örnek: OS = DDoS Saldırısı + Yüksek Ciddiyet

1.5.4 Olayın İzole Edilmesi

- Olayın yayılmasını önlemek amacıyla etkilenen sistemler izole edilmelidir.
- Formül: OI = ES - IS
- Açıklama: ES: Etkilenen Sistemler, IS: İzole Edilen Sistemler
- Örnek: Örnek: OI = Sunucu - İzole Edildi

1.5.5 Müdahale Planı Hazırlama

- Olayın etkilerini minimize etmek ve sistemleri normale döndürmek için bir müdahale planı hazırlanmalıdır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- Formül: MP = MO + RS
- Açıklama: MO: Müdahale Önlemleri, RS: Risk Seviyesi
- Örnek: Örnek: MP = Sunucu Koruma + Orta Risk

1.5.6 Zararın Kontrol Altına Alınması

- Zararın büyümesini engellemek için acil önlemler alınmalıdır.
- Formül: ZK = IZ + AO
- Açıklama: IZ: İzolasyon, AO: Acil Önlemler
- Örnek: Örnek: ZK = Veritabanı İzolasyonu + Erişim Kapatma

1.5.7 Kurtarma Süreci

- Zarar görmüş sistemlerin ve verilerin geri yüklenmesi için kurtarma işlemleri yapılmalıdır.
- Formül: KS = SR + YD
- Açıklama: SR: Sistem Kurtarma, YD: Yedekleme Verileri
- Örnek: Örnek: KS = Sistem Kurtarma + Yedeklerden Geri Yükleme

1.5.8 Olay Sonrası Analiz

- Olayın neden olduğu zarar ve müdahale süreci analiz edilmelidir.
- Formül: OSA = ZA + OA
- Açıklama: ZA: Zarar Analizi, OA: Olayın Analizi
- Örnek: Örnek: OSA = Veritabanı Zarar Analizi + Olayın Detaylı İncelemesi

1.5.9 Güvenlik Zafiyetlerinin Belirlenmesi

- Olay sırasında tespit edilen güvenlik açıkları kayıt altına alınır ve ileride iyileştirme yapılmak üzere listelenir.
- Formül: GZ = SO + AO
- Açıklama: SO: Sistem Açıkları, AO: Alınacak Önlemler
- Örnek: Örnek: GZ = Sunucu Açığı + Firewall Ekleme

1.5.10 İyileştirme Planı

- Gelecekte benzer olayların tekrarlanmasını önlemek için sistem iyileştirme planları hazırlanır.
- Formül: IP = SA + GE
- Açıklama: SA: Sistem İyileştirmeleri, GE: Güvenlik Eklentileri
- Örnek: Örnek: IP = Sunucu Güvenliği + Firewall Yükseltme

1.5.11 Sürekli İzleme ve İyileştirme

- Olay sonrası sistemlerin sürekli olarak izlenmesi ve yeni tehditlere karşı korunması gerekir.
- Formül: SI = IS + GA
- Açıklama: IS: İzleme Sistemleri, GA: Güvenlik Analizleri
- Örnek: Örnek: SI = Ağ İzleme + Güvenlik Kontrolü

1.6 Olay Sonrası İyileştirme Süreci

1.6.1 Güvenlik Açıklarının Analizi

- Siber güvenlik olayının neden meydana geldiği, hangi açıkların kullanıldığı ve sistemdeki zafiyetler analiz edilmelidir.
- Formül: GA = ZA + SO
- Açıklama: ZA: Zarar Analizi, SO: Sistem Açıkları
- Örnek: Örnek: GA = Veritabanı Zarar Analizi + Açık Tespiti

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1.6.2 Güvenlik İyileştirme Planı

- Güvenlik açıklarının tespit edilmesinden sonra, bu açıkların kapatılması ve sistemlerin daha güvenli hale getirilmesi için bir iyileştirme planı hazırlanmalıdır.
- Formül: GIP = SA + AO
- Açıklama: SA: Sistem İyileştirmeleri, AO: Alınacak Önlemler
- Örnek: Örnek: GIP = Sunucu İyileştirmesi + Firewall Eklenmesi

1.6.3 Alınacak Güvenlik Önlemleri

- İyileştirme planında belirlenen güvenlik önlemleri, sistemlerin daha güvenli hale getirilmesi amacıyla alınır.
- Formül: GO = FW + SS
- Açıklama: FW: Firewall, SS: Sistem Sertleştirme
- Örnek: Örnek: GO = Firewall Eklenmesi + Sistem Sertleştirme

1.6.4 Güvenlik Testleri

- İyileştirme sürecinde alınan önlemlerden sonra güvenlik testleri yapılmalıdır.
- Formül: GT = PT + VA
- Açıklama: PT: Penetrasyon Testi, VA: Zayıflık Analizi
- Örnek: Örnek: GT = Penetrasyon Testi + Zayıflık Analizi

1.6.5 Yeni Güvenlik Stratejilerinin Belirlenmesi

- Olay sonrası mevcut güvenlik stratejileri yeniden değerlendirilir ve gelecekte benzer olayların önlenmesi amacıyla yeni stratejiler geliştirilir.
- Formül: GS = PS + NA
- Açıklama: PS: Proaktif Stratejiler, NA: Yeni Altyapı
- Örnek: Örnek: GS = Proaktif Güvenlik Stratejileri + Yeni Altyapı

1.6.6 Eğitim ve Farkındalık Programları

- Çalışanların güvenlik bilincini artırmak amacıyla eğitim ve farkındalık programları düzenlenmelidir.
- Formül: EF = ETP + FP
- Açıklama: ETP: Eğitim Programı, FP: Farkındalık Programı
- Örnek: Örnek: EF = Eğitim Programı + Farkındalık Artırma

1.6.7 Yedekleme Stratejilerinin Güncellenmesi

- Olay sonrası, yedekleme politikaları gözden geçirilmeli ve güncellenmelidir.
- Formül: YS = CV + NYP
- Açıklama: CV: Kritik Veriler, NYP: Yeni Yedekleme Politikaları
- Örnek: Örnek: YS = Kritik Veriler + Yeni Yedekleme Politikaları

1.6.8 Güvenlik İzleme Sistemlerinin Geliştirilmesi

- Sürekli güvenlik izleme ve olay tespit sistemlerinin daha etkin çalışması için geliştirilmeler yapılmalıdır.
- Formül: GIS = SI + OT
- Açıklama: SI: Sistem İzleme, OT: Olay Tespiti
- Örnek: Örnek: GIS = Sistem İzleme Geliştirme + Olay Tespiti

1.6.9 Politika ve Prosedürlerin Gözden Geçirilmesi

- Olay sonrası, mevcut güvenlik politikaları ve prosedürler gözden geçirilmeli, gerekli güncellemeler yapılmalıdır.
- Formül: PP = GP + DP
- Açıklama: GP: Güvenlik Politikaları, DP: Dokümantasyon Prosedürleri

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- Örnek: Örnek: PP = Güvenlik Politikaları + Dokümantasyon Prosedürleri

1.6.10 Sürekli Güvenlik İzleme

- Olay sonrası, sistemler sürekli izlenmeli ve potansiyel tehditlere karşı güvenlik analizleri yapılmalıdır.
- Formül: SGI = SI + GA
- Açıklama: SI: Sistem İzleme, GA: Güvenlik Analizleri
- Örnek: Örnek: SGI = Sistem İzleme + Güvenlik Analizleri

1.6.11 Olay Sonrası Raporlama

- Olay sonrası yapılan tüm müdahale, iyileştirme ve izleme süreçleri raporlanmalıdır.
- Formül: OR = OID + RR
- Açıklama: OID: Olay ID Numarası, RR: Raporlama Raporu
- Örnek: Örnek: OR = 00123 + Detaylı Raporlama

1.6.12 Olayın Tekrarlanma Olasılığının Azaltılması

- Yapılan tüm analizler ve iyileştirmeler, gelecekte benzer bir olayın tekrar yaşanma olasılığını azaltmaya yönelik olmalıdır.
- Formül: TA = IR + GS
- Açıklama: IR: İyileştirme Raporu, GS: Güvenlik Stratejileri
- Örnek: Örnek: TA = İyileştirme Raporu + Güvenlik Stratejisi Uygulaması

1.7 Olay Sonrası Raporlama ve Denetim Süreci

1.7.1 Olayın Detaylı Raporlanması

- Olayın ne zaman, nasıl ve hangi sistemleri etkilediği gibi tüm detaylar raporlanır.
- Formül: ODR = OID + DT + ST
- Açıklama: OID: Olay ID Numarası, DT: Detaylı Tarih ve Saat, ST: Etkilenen Sistemler
- Örnek: Örnek: ODR = 00123 + 2024-01-15 14:32 + Kimlik Doğrulama Sistemi

1.7.2 Müdahale ve Kurtarma Aşamalarının Raporlanması

- Müdahale ve kurtarma aşamalarında hangi adımların atıldığı, hangi ekiplerin hangi zaman dilimlerinde müdahale ettiği raporlanmalıdır.
- Formül: MKR = MA + KA + ZM
- Açıklama: MA: Müdahale Aşamaları, KA: Kurtarma Aşamaları, ZM: Zaman Çizelgesi
- Örnek: Örnek: MKR = Sistem Kapatma + Veritabanı Kurtarma + 2 Saat İçinde Tamamlandı

1.7.3 Alınan Güvenlik Önlemlerinin Raporlanması

- Olay sırasında alınan tüm güvenlik önlemleri ve müdahaleler detaylandırılmalıdır.
- Formül: GOR = GO + AS
- Açıklama: GO: Alınan Önlemler, AS: Alınan Sistemik Tedbirler
- Örnek: Örnek: GOR = Firewall Güçlendirme + Erişim Kısıtlaması

1.7.4 Olayın Etkilerinin Analizi

- Olayın organizasyon üzerinde yarattığı etkiler, mali kayıplar ve operasyonel kesintiler analiz edilmelidir.
- Formül: OEA = EK + OK
- Açıklama: EK: Ekonomik Kayıplar, OK: Operasyonel Kayıplar
- Örnek: Örnek: OEA = 20.000 USD Kayıp + 4 Saat Sistem Kesintisi

1.7.5 Denetim Planı Hazırlama

- Olay sonrası güvenlik tedbirlerinin etkinliğini değerlendirmek amacıyla bir denetim planı hazırlanır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- Formül: DP = DA + ZM
- Açıklama: DA: Denetim Aşamaları, ZM: Zaman Çizelgesi
- Örnek: Örnek: DP = Sistem Denetimi + 2 Haftada Tamamlanacak

1.7.6 Denetim Bulgularının Raporlanması

- Denetim sırasında elde edilen bulgular, güvenlik açıkları ve öneriler raporlanmalıdır.
- Formül: DBR = DB + GS
- Açıklama: DB: Denetim Bulguları, GS: Güvenlik Stratejileri
- Örnek: Örnek: DBR = Veritabanı Açığı Tespit Edildi + Güvenlik Stratejisi Uygulandı

1.7.7 İyileştirme Önerilerinin Sunulması

- Denetim raporunda yer alan güvenlik açıklarına karşı alınabilecek önlemler ve iyileştirme önerileri sunulmalıdır.
- Formül: IO = GZ + İP
- Açıklama: GZ: Güvenlik Zafiyetleri, İP: İyileştirme Planı
- Örnek: Örnek: IO = Şifreleme Eksikliği + Yeni Şifreleme Yöntemi Uygulaması

1.7.8 Olay Sonrası İyileştirme Denetimi

- Olay sonrasında yapılan iyileştirmelerin etkinliği izlenmeli ve ikinci bir denetim yapılmalıdır.
- Formül: OİD = İS + GB
- Açıklama: İS: İyileştirme Sonuçları, GB: Güvenlik Bulguları
- Örnek: Örnek: OİD = Güvenlik Duvarı İyileştirildi + Yeni Açık Yok

1.7.9 Yasal Düzenlemelere Uygunluk Denetimi

- Olay sonrası yapılan müdahaleler ve raporlamalar, yasal düzenlemelere uygun olup olmadığı konusunda denetimden geçmelidir.
- Formül: YDUD = YG + RD
- Açıklama: YG: Yasal Gereklilikler, RD: Raporların Doğruluğu
- Örnek: Örnek: YDUD = KVKK Uygulandı + Raporlar Onaylandı

1.7.10 Denetim Sonuçlarının Raporlanması

- Tüm denetim sonuçları belgelenmeli ve üst yönetimle paylaşılmalıdır.
- Formül: DSR = DSB + ÜY
- Açıklama: DSB: Denetim Sonuç Bulguları, ÜY: Üst Yönetim
- Örnek: Örnek: DSR = Tüm Açıklar Kapandı + Üst Yönetim Bilgilendirildi

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

2. Siber Güvenlik Tedbirleri, Suçların Önlenmesi İçin Kritik Rol Oynar

Siber güvenlik, dijital dünyada var olan tehditlerin, saldırıların ve suçların önlenmesinde önemli bir rol oynar. Özellikle sağlık sektörü gibi hassas veri alanları, bu tehdidin muhafaza edilmesi için oluşturulan yalnızca veri miktarını sağlamakla kalır, aynı zamanda suçların ve yasa dışı faaliyetlerin geçilmesine kadar katkı sağlanır. Siber suçların korunması için uygulanan güvenlik prosedürleri, bu tür olayların yaşanması azalır ve zararlıların bu tür faaliyetlerinde bulunmamaları zorlaştırılır. Aşağıda siber güvenlik önlemlerinin suçlarının önlenmesinde nasıl kritik bir rol oynadığına dair detaylar yer alıyor.

2.1 Güvenlik Duvarları ve İleri Düzey Koruma Sistemleri

Güvenlik duvarları (güvenlik duvarı), bilgisayar sistemlerine ve ağlara yetkisiz erişimi engelleyen bir güvenlik önlemidir. Sağlık sektörü gibi büyük verilerin depolandığı ve işlendiği geniş güvenlik duvarları, dış tehditlerin engellenmesinde kritik b

- **Örnek:** Bir sağlık anlaşması, internet üzerinden gelen ve iç ağa yönlendirilen tüm hatları izleyen ve kötü niyetli yazılımları tespit edip engell

2.2 Şifreleme Teknikleri ve Veri Koruma

Şifreleme, dijital veriler, yetkisiz erişim

- **Örnek:** Bir hastane, hastaların bazılarını şifreleyerek veri dosyalarını saklamaktadır. Veriler şifrelenmişse, yetkisiz bir kullanıcı bu erişim hakkıyla bile bilgilerini çözemeyecektir.

2.3 Kimlik Doğrulama ve Çok Faktörlü Kimlik Doğrulama (MFA)

Kimlik şifresi, bir sistem ya da kullanıma erişim sağlamak isteyen kullanıcıların kimliklerinin doğrulanması işlemi

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Bir doktor, hastane sistemine giriş yaparken sadece kullanıcı adı ve şifre ile değil, ayrıca cep telefonuna gelen bir doğrulama kodunu da girmek zorundadır. Bu yöntem, şifresi ele geçirilen bir doktorun hesabına yetkisiz kişilerin erişmesini engeller.

2.4 Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)

Saldırı tespit sistemleri (IDS), ağ ve sistemlerdeki anormal aktiviteleri izleyerek olası saldırıları belirler. Saldırı önleme sistemleri (IPS) ise bu tespit edilen saldırılara karşı otomatik önlemler alarak saldırıyı engeller. Sağlık kuruluşları gibi hassas veriler barındıran sistemlerde IDS ve IPS, saldırıların erken tespit edilmesinde ve önlenmesinde önemli bir rol oynar. Bu sistemler, kötü niyetli yazılımların veya saldırganların sisteme zarar vermeden önce belirlenmesine ve etkisiz hale getirilmesine olanak tanır.

- **Örnek:** Bir hastane ağına yönelik anormal bir trafiği tespit eden IDS, bu hareketin bir DDoS saldırısı olduğunu belirler ve IPS, trafiği otomatik olarak engelleyerek hastane ağına zarar vermeden saldırıyı durdurur.

2.5 Veri Yedekleme ve Felaket Kurtarma Planları

Veri yedekleme, bir sistemdeki verilerin kaybolması veya zarar görmesi durumunda verilerin geri yüklenmesi için düzenli olarak yedeklenmesi işlemidir. Felaket kurtarma planları ise bir siber saldırı, doğal afet veya sistem arızası gibi durumlarda sistemlerin nasıl tekrar işlevsel hale getirileceğini belirler. Sağlık kuruluşlarında bu tür önlemler, hasta verilerinin kaybolmasını veya erişilemez hale gelmesini engellemek için kritik önem taşır.

- **Örnek:** Bir sağlık kuruluşu, hasta verilerini haftalık olarak yedekler ve bu yedekleri bulut ortamında saklar. Bu sayede bir fidye yazılımı saldırısı olsa dahi, yedeklenen veriler sayesinde hastane kısa sürede normale dönebilir.

2.6 Kullanıcı Farkındalığı ve Eğitim Programları

Siber suçların önlenmesinde teknolojik önlemler kadar önemli olan bir diğer konu da kullanıcı farkındalığıdır. Çalışanlar, siber saldırılar ve tehditler konusunda bilinçlendirilmediği sürece en iyi güvenlik önlemleri bile yeterli olmayabilir. Bu nedenle, sağlık kuruluşları düzenli olarak kullanıcı farkındalığı eğitimleri düzenler. Bu eğitimlerde, phishing saldırıları, güvenli şifre oluşturma ve siber tehditlerle başa çıkma yöntemleri öğretilir.

- **Örnek:** Bir hastane, çalışanlarına düzenli olarak siber güvenlik farkındalık eğitimleri verir. Bu eğitimler sayesinde çalışanlar, e-posta ile gelen phishing saldırılarını tanımakta ve güvenli şifre kullanımı hakkında bilgi sahibi olmaktadır.

2.7 Düzenli Denetimler ve Güvenlik Testleri

Siber suçların önlenmesinde bir diğer kritik unsur da düzenli olarak yapılan güvenlik denetimleri ve testlerdir. Penetrasyon testleri (pentest) gibi güvenlik testleri, sistemlerdeki olası zafiyetleri belirleyerek bu zafiyetlerin bir saldırı gerçekleşmeden önce giderilmesine olanak tanır. Düzenli güvenlik denetimleri ise sağlık kuruluşlarının bilgi güvenliği politikalarının etkinliğini değerlendirir.

- **Örnek:** Bir hastane, düzenli olarak penetrasyon testleri yaptırır ve bu testlerin sonuçlarına göre sistemdeki güvenlik açıklarını kapatır. Ayrıca, düzenli denetimlerle bilgi güvenliği politikalarının etkinliği kontrol edilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

*****Siber güvenlik tedbirleri, sadece verilerin korunmasını sağlamakla kalmaz, aynı zamanda suçların işlenmesini zorlaştırarak suçların önlenmesinde kritik bir rol oynar. Güvenlik duvarları, şifreleme teknikleri, kimlik doğrulama sistemleri, saldırı tespit ve önleme mekanizmaları gibi çeşitli teknik önlemler, sağlık sektöründe siber suçlara karşı güçlü bir savunma sağlar. Ayrıca, kullanıcı farkındalığı eğitimleri, düzenli denetimler ve felaket kurtarma planları gibi stratejiler de siber suçlarla mücadelede önemli katkılar sunar.*****

3. Hukuki Düzenlemeler Siber Suçlara Karşı Caydırıcı Olmalıdır

Siber suçlar, dijital dünyada her geçen gün artan bir tehdit haline geldi. Özellikle sağlık sektörü gibi hassas verilerin saklanması

3.1 Siber Suçların Hukuki Tanımı

Siber suçlar, dijital sistemler aracılığıyla işlenen suçlar olarak çözümler. Bu suçlar arasında veri hırsızlığı, sisteme yetkisiz erişim, fidye yazılım saldırıları, kimlik hırsızlığı, sahtekarlık ve veri manipülasyonu gibi eylemler yer alır. Ülkenin hukuk sistemi

Örnek: Türkiye'de kişisel verilerin korunması kanunu (KVKK) kapsamında siber suçlar, kişisel verilerin hukuka aykırı şekilde elde edilmesi, paylaşılması ve

3.2 Caydırıcı Cezai Yaptırımlar

Siber suçlarla mücadel

- **Ağır Cezalar:** Kişisel sağlık verilerinin çalınması veya kötü şekilde
- **Örnek:** Bir sağlık sistemine fidye yazılım saldırıları kişilerin hapis cezasına çarptırılması, siber suçluların gözlerinin korkutulması mümkündür.

3.3 Uluslararası Hukuki İşbirliği ve Veri Paylaşımı

Siber suçlar çoğu zaman sınır tanımadan uluslararası boyutta işlenir. Bu nedenle, yalnızca ulusal düzeydeki hukuki yapılar yeterli değildir. Uluslararası işbirliği ve bilgi paylaşımı, siber suçluların tespit edilmesi ve yargılama açısından kritik öneme sahiptir. Özellikle sağlık sektöründe, uluslararası veri transferleri sırasında işlenen suçlarda ülkeler arası işbirliği h

- **Örnek:** Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), kişisel verilerin korunmasına ilişkin uluslararası düzenlemeleri içerir. GDPR çerçevesinde, bir Avrupa'da işlenen siber suçun başarısızlığının başka bir ülkede yakalanması durumunda hukuki işbirliği yapılır.

3.4 Düzenleyici Kurumlar ve Denetim Mekanizmaları

Siber güvenliğin sürdürülmesinde sağlayıcı kurumlarda büyük bir rol oynar. Bu kurumlar, siber suçların büyümesi, raporlanması ve suçluların sınıflandırılması sırasında aktif olarak yer alır. Düzenleyici kurumlar ayrıca, ülkeler ve kamu kurumlarının siber güvenlik politikalarının denetimini denetler ve cezai işlemleri başlatır.

- **Örnek:** Türkiye'de Kişisel Verileri Koruma Kurumu (KVKK), sağlık sektörünün veri politikalarını denetler ve gerekli önlemlerin alındığı kuruluşlara idari para cezası uygular.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

3.5 Siber Suçların Takibi ve Hukuki Süreçler

Siber suçlar genellikle karmaşık yapılarla işlenir ve suçluların sürülmesine izin verilmesi zordur. Bu nedenle, siber suçların yapısı ve hukuki sürecin yürütülmesi için etkin bir takip sistemi gereklidir. Siber suçların, saldırıların nasıl ve kim tarafından gerçekleştirildiğini tespit etmek için dijital adli tıp ve siber izleme araçları kullanılır. Bu araçların, suçluların adalet karşısında ortaya çıkmasında hayati bir rol oynar.

- **Örnek:** Bir sağlık durumu, fidye yazılım saldırısına durumunda, dijital adli tıp ekipleri saldırılarının bozulmalarını tespit etmek için sistem üzerinde incelemeler yapar ve delil toplar. Bu deliller, hukuki durumlarda suçluların yargılanması için kullanılır.

3.6 Yasalara Uygun Veri Toplama ve Adli Delil Yönetimi

Siber suçların yargılanması için delil toplama

- **Örnek:** Bir hastaneye yönelik gerçekleştirilen bir saldırının ardından, saldırının detaylarını içeren loglar ve diğer dijital izler yasal delil olarak toplanır. Bu verilerin güvenliği, adli süreçlerin sağlıklı yürütülmesi için son derece önemlidir.

3.7 Bilgi Güvenliği Yönetim Sistemlerinin Yasal Zorunluluğu

Sağlık kuruluşları ve diğer büyük kurumlar, bilgi güvenliği yönetim sistemlerini (BGYS) kurmak ve düzenli olarak bu sistemleri güncellemekle yükümlüdür. Bu sistemlerin yasal bir zorunluluk haline getirilmesi, siber suçların önlenmesinde etkin bir rol oynar. BGYS, kurumların siber güvenlik politikalarını belirlemelerini, bu politikaları uygulamalarını ve denetlemelerini sağlar.

- **Örnek:** Türkiye'de KVKK kapsamında, sağlık sektöründeki büyük kuruluşlar bilgi güvenliği yönetim sistemlerini kurmak ve düzenli olarak raporlamak zorundadır. Bu zorunluluk, verilerin korunmasında önemli bir adım olarak görülmektedir.

3.8 Hukuki Düzenlemelerin Güncellenmesi ve Teknolojiye Uyum

Teknolojik gelişmeler, yeni siber tehditlerin ortaya çıkmasına yol açar. Bu nedenle, hukuki düzenlemelerin de güncel tehditler ve yeni teknolojilere uyumlu olacak şekilde sürekli olarak güncellenmesi gerekir. Siber suçlarla mücadelede yetersiz kalan yasalar, suçluların yeni yöntemler kullanarak güvenlik açıklarını istismar etmesine olanak tanır. Teknolojik gelişmelere uyumlu yasalar, siber suçların önlenmesinde daha etkili bir rol oynar.

- **Örnek:** 2020 yılında Türkiye'de yapılan KVKK güncellemeleri, fidye yazılımları ve veri ihlalleri gibi yeni tehditler göz önünde bulundurularak düzenlenmiştir. Bu güncellemeler, teknolojinin ilerlemesiyle ortaya çıkan yeni saldırı vektörlerine karşı daha güçlü yasal koruma sağlar.

3.9 Etik ve Hukuki Sorumlulukların Dengesi

Siber suçların önlenmesi ve cezalandırılması sürecinde yalnızca hukuki düzenlemeler değil, aynı zamanda etik ilkeler de göz önünde bulundurulmalıdır. Hukuki yaptırımların caydırıcılığı, toplumsal güvenlik ve kişisel hakların korunmasıyla dengelenmelidir. Ayrıca, sağlık sektöründe etik sorumlulukların yerine getirilmesi, siber güvenlik önlemleri ile birlikte ele alınmalıdır.

- **Örnek:** Bir hastane, veri güvenliğini sağlamak adına aldığı önlemleri hukuki ve etik sorumluluklarla uyumlu şekilde yürütür. Hasta bilgilerinin gizliliği korunurken, hasta hakları da göz önünde bulundurulur.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

Siber suçlara karşı caydırıcı hukuki düzenlemeler, dijital dünyada suçların önlenmesi ve suçluların adalet önüne çıkarılması için kritik bir role sahiptir. Cezai yaptırımların sertleştirilmesi, uluslararası işbirliği, düzenleyici kurumların etkin çalışması ve yasalara uygun veri toplama süreçleri, siber suçlarla mücadelede etkili yöntemlerdir. Bu düzenlemelerin teknolojiyle uyumlu bir şekilde güncellenmesi ve etik sorumluluklarla dengelenmesi, dijital dünyanın daha güvenli hale gelmesine katkı sağlar.

4. İnsanlar ve Kurumlar İçin Bilinçlenme Önemlidir

Siber güvenlik, yalnızca teknik sınırlara sahip olmayan geniş bir listedir. Bilgisayar sistemleri ve dijital altyapılar ne kadar güvenli hale getirilirse, insan faktörü güvenlik zincirinin en zayıf halka olabilir. Bu nedenle, siber tehditlerin karşısında durmak ve bireylerin bilinçlenmesi, hem bireysel güvenlik hem de kurumsal güvenliğin sürdürülme açısından büyük önem taşır. Bilinçlenme, durdurulacak ve insanların siber tehdidi

A

4.1 İnsan Faktörünün Siber Güvenlikteki Rolü

İnsan faktörü, siber güvenlik

- **Örnek:** Bir hastane çalışanları, güvenli olmayan

4.2 Bilinçlenme Eğitimlerinin Önemi

Kurumlar, siber güvenlik

- **Türkçe:** Bir sağlık kurulu

4.3 Sosyal Mühendislik ve Bilinçsiz Kullanım Riskleri

Sosyal müh

- **Türkçe: Örnek:** Bir dolandırıcı,

4.4 Kurumsal Siber Güvenlik Politikalarının Uygulanması

Kurumlar, çalışanlarının si

- **Örnek:** Bir banka, çalışanları için siber güvenlik politikaları oluşturur. Bu politikalar, çalışanların şifrelerini düzenli olarak değiştirmeleri, hassas verilere erişim yetkisi olan kişilerin belirlenmesi ve çalışanların yalnızca güvenli ağlar üzerinden sisteme erişim sağlamaları gerektiğini belirtir.

4.5 Bilinçlenme, Veri Güvenliği İhlallerinin Önlenmesine Katkı Sağlar

Bireylerin ve kurumların siber güvenlik konusunda bilinçli olması, veri ihlallerinin ve veri sızıntılarının önlenmesinde önemli bir rol oynar. Bireyler, verilerini nasıl koruyacaklarını ve hangi yöntemlerle güvence altına alacaklarını bildiklerinde, kişisel ve kurumsal verilerin siber saldırganlar tarafından ele geçirilmesi daha zor hale gelir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Bir sağlık kuruluşu, hasta bilgilerinin güvenliğini sağlamak için çalışanlarına veri şifreleme ve erişim kontrolü konusunda bilinçlendirme eğitimleri verir. Bu eğitimler sayesinde çalışanlar, verilerin yalnızca yetkili kişilere açık olmasını sağlar ve veri ihlallerinin önüne geçer.

4.6 Bilinçli Parola Kullanımı ve Güvenlik Protokollerinin Önemi

Siber güvenlik ihlallerinin büyük bir kısmı, zayıf parola kullanımı ve güvenlik protokollerinin ihmal edilmesinden kaynaklanır. Güçlü ve benzersiz parolaların kullanılması, çok faktörlü kimlik doğrulama (MFA) yöntemlerinin benimsenmesi ve güvenlik protokollerinin titizlikle uygulanması, bireylerin ve kurumların siber tehditlere karşı korunmasına katkı sağlar.

- **Örnek:** Bir çalışan, aynı zayıf parolayı hem kişisel hesaplarında hem de iş e-posta hesaplarında kullanarak bir güvenlik zafiyetine neden olabilir. Ancak, siber güvenlik bilincine sahip olan çalışanlar, her hesap için farklı ve güçlü parolalar oluşturur ve bu parolaların korunması için çok faktörlü kimlik doğrulama (MFA) yöntemlerini kullanır.

4.7 Sosyal Medya ve İnternet Kullanımı Konusunda Farkındalık

Günümüzde sosyal medya ve internet kullanımı hızla artmaktadır, bu da siber suçlular için yeni bir saldırı alanı yaratır. Sosyal medyada paylaşılan bilgilerin dikkatlice yönetilmesi ve internette güvenli olmayan sitelere karşı farkındalığın artırılması gerekmektedir. Bireylerin sosyal mühendislik saldırılarına karşı dikkatli olmaları ve kişisel bilgilerini açık şekilde paylaşmamaları önemlidir.

- **Örnek:** Bir çalışan, sosyal medya üzerinden fazla kişisel bilgi paylaşarak bir saldırganın sosyal mühendislik yöntemleriyle bu bilgileri kullanmasına olanak tanıyabilir. Ancak, bilinçli kullanıcılar, sosyal medyada paylaştıkları bilgilerin miktarını sınırlandırarak kendilerini bu tür saldırılara karşı korur.

4.8 Düzenli Testler ve Denetimlerle Bilinçlenme Sürecinin Güçlendirilmesi

Siber güvenlik bilinci sadece eğitimlerle değil, aynı zamanda düzenli testler ve denetimlerle de desteklenmelidir. Kurumlar, çalışanlarının siber güvenlik tehditlerine karşı nasıl tepki verdiklerini görmek için düzenli güvenlik testleri yapmalı ve sonuçlara göre bilinçlenme eğitimlerini güncellemelidir. Denetimlerin düzenli olarak yapılması, güvenlik açıklarının tespit edilmesine ve giderilmesine olanak sağlar.

- **Örnek:** Bir sağlık kuruluşu, çalışanlarına belirli aralıklarla phishing testleri yapar. Bu testlerde, çalışanlara sahte e-postalar gönderilir ve bu tür tehditlere karşı verdikleri tepkiler değerlendirilir. Test sonuçlarına göre, bilinçlendirme eğitimleri düzenlenir.

4.9 Yönetici ve Liderlik Rolündeki Kişilerin Bilinçlendirilmesi

Siber güvenlik bilincinin sadece çalışan düzeyinde kalmaması, aynı zamanda yönetici ve lider pozisyonunda bulunan kişilere de aktarılması gerekmektedir. Kurum yöneticileri, alınan siber güvenlik tedbirlerini anlayarak ve destekleyerek tüm kurumun güvenlik politikasını benimsemelidir. Yönetim katmanındaki bilinçlenme, tüm kurum genelinde güvenlik önlemlerinin etkin bir şekilde uygulanmasını sağlar.

- **Örnek:** Bir hastane yönetimi, düzenli olarak siber güvenlik konusunda bilgilendirme toplantıları yapar ve hastane genelinde uygulanan güvenlik politikalarını destekler. Yönetim katmanında alınan bilinçli kararlar, tüm sağlık personelinin bu politikaları daha ciddiye almasını sağlar.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

İnsanların ve kurumların siber güvenlik bilincine sahip olması, dijital dünyanın giderek artan tehditlerine karşı etkili bir savunma oluşturur. Eğitimler, farkındalık programları, düzenli testler ve güvenlik politikalarının uygulanması, hem bireylerin hem de kurumların güvenliklerini artırır. Siber tehditler karşısında bilinçli bir şekilde hareket eden bireyler ve çalışanlar, suçların önlenmesine katkıda bulunarak dijital ortamları daha

5. Uluslararası İşbirliği Gerekli

Siber suçlar,

Aşağıda uluslararası işbirliğinin

5.1 Siber Suçların Sınır Tanımayan Yapısı

Siber suçlar, çoğu

- **Örnek:** Avrupa'dan bir sağlık

5.2 Uluslararası Hukuki Düzenlemelerin Uyumlaştırılması

Ülkenin kendi siber güvenlik politikaları ve düzenlemeleri vardır. Ancak ülkeler

- **Örnek:** Avrupa B

5.3 Bilgi Paylaşımı ve Siber Tehdit İstihbaratı

Uluslararası işbirliğinin bir

- **Türkçe: Örnek:** Bir sağlık sistemine yöneldik

5.4 Ortak Siber Güvenlik Stratejilerinin Geliştirilmesi

Siberler

- **Örnek:** NATO'nun siber savunması

5.5 Siber Suçlarla Mücadelede Uluslararası Anlaşmalar

Uluslararası düzeyde siber suçlarla mücadele etmek için birçok ülke arasında imzalanan anlaşmalar ve protokoller bulunmaktadır. Bu anlaşmalar, ülkeler arasında siber suçluların seçimi, veri güvenliği standartlarının belirlenmesi ve hukuki boyutların genişletilmesi gibi konuları içermektedir. Uluslararası siber güvenlik anlaşmaları, ülkelerin birlikte hareket etmelerini sağlayarak suçluların adaletten kaçmasını zorlaştırır.

- **Örnek:** Budapeşte Siber Suçlar Sözleşmesi (Cybercri)

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

5.6 Kurumsal İşbirliği ve Özel Sektör Katılımı

Uluslararası işbirliği sadece devletler düzeyinde değil, aynı zamanda özel sektör düzeyinde de yapılmalıdır. Özel sektör şirketleri, özellikle teknoloji ve sağlık sektöründe faaliyet gösteren büyük kuruluşlar, siber tehditlerin hedefindedir. Bu nedenle, özel sektör ve devletler arasında siber güvenlik alanında işbirliği yapılması, ortak güvenlik stratejilerinin geliştirilmesi ve bilgi paylaşımı çok önemlidir.

- **Örnek:** Bir sağlık kuruluşu, uluslararası teknoloji şirketleriyle işbirliği yaparak güvenlik açıklarını kapatmak ve daha güvenli sistemler oluşturmak amacıyla yeni teknolojiler geliştirir.

5.7 Siber Saldırıların Kaynağının Tespit Edilmesi

Birçok siber saldırı, farklı ülkelerde bulunan saldırı altyapıları (botnet'ler, proxy sunucuları vb.) kullanılarak gerçekleştirilir. Bu nedenle, saldırıların kaynağını tespit etmek ve saldırganları adalet önüne çıkarmak için uluslararası düzeyde teknik işbirliği gereklidir. Siber saldırıların kaynağını bulmak, suçluların izlerini takip etmek ve bu suçların tekrarlanmasını engellemek açısından önemlidir.

- **Örnek:** Bir sağlık kuruluşuna yönelik DDoS saldırısının kaynağını bulmak için uluslararası bir siber güvenlik ekibi, saldırının hangi sunuculardan gerçekleştirildiğini tespit eder ve bu sunucuların bulunduğu ülkelerle işbirliği yaparak saldırıyı durdurur.

5.8 Siber Tatbikatlar ve Acil Durum Planları

Siber tatbikatlar ve acil durum planları, siber güvenlik alanında hazırlıklı olunması

5.8.1 Siber Tatbikatların Önemi

Siber tatlılar, gerçek bir saldırı ortamını simüle ederek kurumsal ve ül

- **Örnek:** Bir sağlık kuruluşu, fidye yazılımı saldırısını simüle eden bir tatbikat düzenler. Tatbikat sırasında, çalışanlar saldırıya karşı nasıl tepki vereceklerini öğrenir, teknik ekipler veri yedekleme süreçlerini test eder ve yönetim kadrosu acil durum iletişim planını devreye sokar. Tatbikat sonrası yapılan değerlendirmede, kurumun zayıf noktaları belirlenir ve bu açıkları kapatmak için gerekli adımlar atılır.

5.8.2 Acil Durum Planları

Siber saldırıların meydana geldiği durumlarda, hızlı ve etkin bir müdahale büyük önem taşır. Acil durum planları, siber saldırı anında ve sonrasında izlenecek adımları belirleyen bir kılavuz niteliğindedir. Bu planlar, saldırının etkilerini en aza indirmeyi, kritik sistemleri korumayı, veri kaybını önlemeyi ve kurumun normal operasyonlarına hızlı bir şekilde geri dönmesini sağlamayı amaçlar. Sağlık sektöründe acil durum planları, hasta verilerinin korunması ve hizmetlerin kesintisiz devam edebilmesi açısından hayati bir öneme sahiptir.

- **Örnek:** Bir hastane, veri sızıntısı riski taşıyan bir saldırı sonrası, acil durum planını devreye sokar. Plan kapsamında, hastanenin IT ekibi önce sistemleri izole eder, daha sonra veri yedekleme sistemlerini devreye alır ve hasta kayıtlarına sadece belirli yetkililerin erişmesini sağlar. Bu süreçte kriz iletişim ekibi, hastane yönetimi ile sağlık çalışanlarını bilgilendirir ve dışarıya bilgi sızmasını engeller.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

5.8.3 Tatbikat Türleri

Siber tatbikatlar, çeşitli türlerde düzenlenebilir. Tatbikatlar genellikle gerçekçi saldırı senaryoları temel alınarak hazırlanır ve saldırının etkileri, ekiplerin performansı ve saldırıya karşı alınan önlemler değerlendirilir. Farklı tatbikat türleri, kurumların farklı saldırı türlerine karşı ne kadar hazırlıklı olduğunu test eder.

- **Masa Başı Tatbikatı (Tabletop Exercise):** Bu tür tatbikatlar, teorik bir saldırı senaryosu üzerinden yapılır ve ekiplerin saldırıya nasıl tepki vereceklerini simüle eder. Tatbikat sırasında teknik bir müdahale yapılmaz, ancak stratejik karar alma ve yönetim becerileri test edilir.
- **Simülasyon Tatbikatları (Simulated Attack Exercises):** Bu tatbikatlarda, gerçek bir siber saldırı simüle edilir. Ağ ve sistemler üzerindeki saldırılar, teknik ekiplerin müdahalesini gerektirir ve bu süreçte teknik beceriler test edilir. Simülasyon tatbikatları, gerçek bir saldırı ortamına yakın koşullarda yapılır.
- **Bütünleşik Tatbikatlar (Integrated Exercises):** Bu tatbikatlar, hem teknik ekiplerin hem de yönetim kadrosunun dahil olduğu, kapsamlı ve karmaşık saldırı senaryolarını içerir. Saldırıya karşı teknik müdahaleler yapılırken, aynı zamanda kurum içi iletişim, kriz yönetimi ve operasyonel süreklilik planları test edilir.

5.8.4 Uluslararası Tatbikatlar

Siber saldırılar genellikle sınır tanımadığı için, uluslararası işbirliğini test eden tatbikatlar büyük önem taşır. Bu tatbikatlar, birden fazla ülkenin katılımıyla düzenlenir ve ülkeler arası bilgi paylaşımı, kriz yönetimi ve siber savunma stratejileri test edilir. Uluslararası siber tatbikatlar, özellikle kritik altyapılara yönelik büyük ölçekli saldırılarda ülkelerin nasıl işbirliği yapacağını görmek açısından önemlidir.

- **Örnek:** NATO öncülüğünde düzenlenen bir siber tatbikatta, birden fazla ülkenin sağlık altyapısına yönelik büyük bir DDoS saldırısı simüle edilir. Tatbikat sırasında, katılımcı ülkeler arası bilgi paylaşımı yapılır, saldırıya karşı alınacak önlemler koordineli bir şekilde uygulanır ve saldırının etkileri analiz edilir.

5.8.5 Tatbikat Sonrası Değerlendirme

Tatbikatların en önemli aşamalarından biri, tatbikat sonrasında yapılan değerlendirmelerdir. Bu değerlendirmeler, tatbikat sırasında tespit edilen zayıflıkları ve güçlü yanları analiz eder. Tatbikat sonrası raporlar, kurumların hangi alanlarda iyileştirme yapması gerektiğini gösterir ve bu alanlarda alınacak önlemleri belirler. Ayrıca, tatbikatın nasıl geçtiğini ve ekiplerin performansını ölçen bu raporlar, gelecekte yapılacak tatbikatlar için yol gösterici olur.

- **Örnek:** Bir hastane, fidye yazılımı tatbikatı sonrası, veri yedekleme süreçlerinin yeterince hızlı olmadığını tespit eder. Tatbikat değerlendirmesi sonucunda, yedekleme altyapısını güçlendirme kararı alır ve bir sonraki tatbikatta bu alandaki gelişmeleri test eder.

5.8.6 Sürekli İyileştirme ve Hazırlık

Siber tehditler sürekli olarak evrim geçirir. Bu nedenle, siber tatbikatlar sadece bir kez yapılmamalı, düzenli aralıklarla tekrarlanmalıdır. Sürekli yapılan tatbikatlar, kurumların ve ülkelerin siber tehditlere karşı hazırlıklı olmasını sağlar. Ayrıca, her tatbikattan elde edilen deneyimlerle, acil durum planları ve güvenlik önlemleri sürekli olarak iyileştirilmeli ve güncellenmelidir.

- **Örnek:** Bir sağlık kuruluşu, her yıl düzenli olarak siber tatbikatlar gerçekleştirir. Tatbikat sonuçlarına göre acil durum planlarını günceller, yeni ortaya çıkan tehditlere karşı güvenlik politikalarını revize eder ve ekiplerin yetkinliklerini artırmak için ek eğitimler düzenler.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

Siber tatbikatlar ve acil durum planları, siber güvenlik alanında hazırlıklı olmanın temelini oluşturur. Bu tatbikatlar, kurumların siber saldırılara karşı nasıl tepki vereceğini test ederken, acil durum planları ise saldırı anında ve sonrasında uygulanacak adımları belirler. Tatbikatlar ve acil durum planları sayesinde siber saldırıların etkileri minimize edilir, sistemlerin hızlı bir şekilde normale dönmesi sağlanır ve gelecekteki saldırılara karşı daha güçlü bir savunma hattı oluşturulur.

Sonuç

Uluslararası işbirliği, siber suçlarla mücadelede ve küresel siber güvenliğin sağlanmasında kritik bir rol oynar. Siber suçların sınır tanımayan yapısı, hukuki düzenlemelerin uyumlaştırılması, bilgi paylaşımı, ortak stratejilerin geliştirilmesi ve uluslararası anlaşmalar sayesinde etkili bir şekilde önlenebilir. Hem devletler hem de özel sektör arasında gerçekleştirilen işbirlikleri, siber tehditlere karşı güçlü bir savunma oluşturulmasına katkı sağlar. Siber güvenlik, küresel çapta bir işbirliği gerektirir ve bu işbirliği olmadan siber suçlarla mücadelede etkili sonuçlar elde etmek mümkün değildir.

Siber Güvenlik ve Bilinçlenmenin Kritik Önemi

Siber güvenlik, modern dijital dünyada bireylerin, kurumların ve hatta ulusların karşılaştığı en büyük tehditlerden biri haline gelmiştir. Bilgisayar ağlarının, dijital altyapıların ve hassas verilerin korunması, hem kişisel gizlilik hem de ulusal güvenlik açısından hayati bir önem taşır. Ancak, siber tehditlere karşı sadece teknik çözümler ve güvenlik önlemleri almak yeterli değildir; aynı zamanda, insanların ve kurumların siber tehditler hakkında bilinçlenmesi, bu tehditlere karşı ne kadar hazır olduklarını belirleyen kritik bir faktördür.

Bu kapsamda, siber güvenlik alanında bilinçlenme, uluslararası işbirliği, siber tatbikatlar ve acil durum planları gibi birçok konu detaylı olarak ele alınmıştır. Bu konuların her biri, siber güvenliğin sağlanması ve siber suçların önlenmesinde önemli rol oynar. Aşağıda, bu konuların genel bir değerlendirmesi ve siber güvenlik stratejisinin nasıl geliştirilmesi gerektiğiyle ilgili detaylı sonuçlar yer almaktadır.

1. Bilinçlenme, İnsan ve Kurumların Güvenlikteki En Büyük Gücü

Siber güvenlikte bilinçlenme, en az teknik çözümler kadar önemlidir. İnsan faktörü, siber suçlar karşısında hem en zayıf halka hem de en güçlü savunma olabilir. Çalışanların ve bireylerin siber tehditler hakkında bilgilendirilmesi, siber suçluların işini zorlaştırır ve potansiyel tehditlerin önüne geçer. Kurumlar, çalışanlarına düzenli olarak bilinçlendirme eğitimleri düzenlemeli, özellikle phishing, sosyal mühendislik ve zayıf parola kullanımı gibi yaygın saldırılara karşı farkındalık kazandırmalıdır. Bilinçlenme sayesinde, güvenlik açıklarının büyük bir bölümü daha saldırı gerçekleşmeden kapatılabilir.

- **Sonuç:** Kurumlar, düzenli bilinçlendirme eğitimleri vererek çalışanlarının siber güvenlik farkındalığını artırmalı ve insan faktörünü güvenlik zincirinin en güçlü halkası haline getirmelidir.

2. Siber Güvenlik Tedbirleri Suçların Önlenmesinde Kritik Rol Oynar

Teknolojik çözümler, siber suçların önlenmesi ve güvenlik açıklarının kapatılmasında vazgeçilmezdir. Güvenlik duvarları, şifreleme teknikleri, kimlik doğrulama sistemleri ve saldırı tespit sistemleri gibi teknik önlemler, siber saldırılara karşı birincil savunma hattını oluşturur. Ancak bu önlemlerin etkin olabilmesi için sürekli olarak güncellenmeleri ve yeni tehditlere karşı adapte edilmeleri gerekmektedir. Ayrıca, veri yedekleme ve felaket kurtarma planları da saldırı sonrası verilerin kurtarılması ve sistemlerin hızlı bir şekilde normale dönmesi açısından büyük önem taşır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Sonuç:** Teknik siber güvenlik tedbirleri, güvenlik zincirinin en önemli halkasıdır. Kurumlar, bu tedbirleri sürekli olarak güncellemeli ve siber tehditlere karşı hazırlıklı olmalıdır.

3. Hukuki Düzenlemeler Caydırıcı Olmalı ve Etkin Uygulanmalı

Siber suçlarla mücadelede hukuki düzenlemeler, caydırıcı bir etkiye sahip olmalıdır. Siber suçlular, hafif yaptırımlarla karşılaşmayacaklarını bilmelidir. Bunun yanı sıra, uluslararası düzeyde uyumlu hukuki çerçeveler oluşturulmalı ve ülkeler arası işbirliği artırılmalıdır. Siber suçların sınır tanımayan yapısı, uluslararası hukuki işbirliğini zorunlu hale getirmektedir. Budapeşte Siber Suçlar Sözleşmesi gibi uluslararası anlaşmalar, ülkeler arası işbirliğinin güçlendirilmesi için önemli adımlardır. Aynı zamanda, düzenleyici kurumlar ve denetim mekanizmaları da siber suçların izlenmesi ve önlenmesi konusunda aktif bir rol üstlenmelidir.

- **Sonuç:** Hukuki düzenlemeler siber suçlarla mücadelede caydırıcı olmalı, uluslararası işbirliği artırılmalı ve düzenleyici kurumlar etkin bir şekilde çalışmalıdır.

4. Uluslararası İşbirliği Siber Güvenlikte Başarı İçin Zorunludur

Siber suçların uluslararası yapısı, küresel işbirliğini zorunlu kılmaktadır. Farklı ülkelerde gerçekleşen saldırılar, sınır ötesi işbirliği ve bilgi paylaşımı olmadan etkili bir şekilde önlenemez. Uluslararası siber güvenlik anlaşmaları, istihbarat paylaşımı, ortak siber güvenlik stratejileri ve uluslararası tatbikatlar gibi uygulamalar, siber suçlarla mücadelede kilit rol oynar. Ülkeler arası işbirliği, sadece suçluların yakalanmasını değil, aynı zamanda kritik altyapıların korunmasını da sağlar.

- **Sonuç:** Uluslararası işbirliği, siber güvenliğin küresel düzeyde sağlanmasında temel bir gerekliliktir. Ülkeler ve kurumlar, siber suçlarla mücadelede daha yakın işbirliği yapmalı ve ortak güvenlik stratejileri geliştirmelidir.

5. Siber Tatbikatlar ve Acil Durum Planları Hazırlıklı Olmayı Sağlar

Siber tatbikatlar ve acil durum planları, kurumların ve ülkelerin siber saldırılara karşı hazırlıklı olmasını sağlar. Gerçek saldırı simülasyonları, güvenlik açıklarının tespit edilmesine, acil durum planlarının test edilmesine ve kurumların olası saldırılar karşısında nasıl tepki vereceğini değerlendirmeye olanak tanır. Ayrıca, düzenli olarak yapılan tatbikatlar, tehditlere karşı alınacak önlemlerin etkinliğini artırır ve siber güvenlik ekiplerinin yetkinliklerini geliştirir. Acil durum planları, özellikle sağlık sektörü gibi kritik alanlarda veri kaybını önlemeye ve operasyonların kesintisiz devam etmesini sağlamaya yardımcı olur.

- **Sonuç:** Düzenli siber tatbikatlar ve acil durum planları, siber saldırılar karşısında hazırlıklı olmanın en etkili yollarından biridir. Kurumlar, bu tatbikatları düzenli olarak gerçekleştirmeli ve acil durum planlarını güncel tutmalıdır.

Genel Değerlendirme

Siber güvenlik, teknik çözümler, bilinçlenme, hukuki düzenlemeler ve uluslararası işbirliği gibi birçok unsurun bir araya gelmesiyle sağlanabilir. Siber tehditler sürekli gelişmekte ve karmaşıklaşmaktadır, bu yüzden kurumlar, bireyler ve devletler bu tehditlere karşı hazırlıklı olmalı ve sürekli olarak kendilerini geliştirmelidir. Bilinçlenme ve eğitim programları, insan faktörünü güvenlik zincirinin en güçlü halkası haline getirebilirken, teknik tedbirler, siber suçların gerçekleşmesini zorlaştırır. Hukuki düzenlemeler ve cezai yaptırımlar, siber suçluların caydırılmasında etkili olurken, uluslararası işbirliği, küresel siber suçlarla mücadelede olmazsa olmaz bir unsurdur.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

Sonuç olarak, siber güvenliğin sağlanması, sadece bir ülkenin veya kurumun tek başına yapabileceği bir şey değildir. Küresel çapta bir işbirliği, sürekli eğitim ve bilinçlenme, güncellenen teknik çözümler ve güçlü hukuki çerçeveler sayesinde, siber güvenlik tehditlerine karşı etkili bir savunma hattı oluşturulabilir.

Gelecekte Siber Güvenlik ve Somut Öngörüler

Sibergü

Aşağı

1. Yapay Zeka ve Makine Öğrenimi Tabanlı Güvenlik Çözümleri

Yapay zeka

- **Örnek:** Bir sağlık politikası, AI tabanlı bir güvenlik sistemi

2. Kuantum Bilgisayarların Siber Güvenlik Üzerindeki Etkisi

Kuant

- **Örnek:** Kuantum bilgisayarların yaygınlaşmasıyla birlikte, bugün kullanılan RSA ve AES gibi yaygın şifrelemeleri gü

3. Blockchain Tabanlı Güvenlik Uygulamaları

Blockchain teknolojisi,

- **Örnek:** Sağlık sektöründe hasta kayıtlarının güv

4. IoT (Nesnelerin İnterneti) Güvenliğinin Artan Önemi

N

- **Örnek:** Bir akıllı şehirde ku

5. Sıfır Güven (Sıfır Güven) Mimarisine Geçiş

Geleneksel güvenlik tedavilerinde, bir kullanıcı

- **Örnek:** Bir şirket, Zero Trust mimarisini benimseyerek tüm kullanıcıların onun oturum açma girişiminde kimlik doğrulaması yapması zorunludur. Aynı zamanda insanların sistemdeki her bir ver

6. 5G Teknolojisinin Getirdiği Güvenlik Zorlukları

5G teknolojisi, daha hızlı ve güvenilir bir internet bağlantısı sağlarken, aynı zamanda daha fazla cihazın internete bağlanmasına olanak sağlar

- **Örnek:** 5G ağı üzerinden

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

7. Büyük Veri ve Analitik Tabanlı Güvenlik Çözümleri

Büyük veri, siber güvenlik tehditlerini daha hızlı tespit etmek ve analiz etmek için kullanılabilir. Gelecekte, büyük veri analitiği ile siber saldırıların tespit edilmesi, saldırıdan önceki işaretlerin izlenmesi ve saldırgan davranışlarının analiz edilmesi mümkün olacaktır. Veri analitiği, siber güvenlik ekiplerine, saldırılara karşı proaktif bir yaklaşım benimsemeleri için önemli ipuçları sunar.

- **Örnek:** Bir sağlık kuruluşu, büyük veri analitiği kullanarak sistemdeki tüm kullanıcı davranışlarını izler ve bu verilerle anormal aktiviteleri tespit eder. Büyük veri analitiği, sistemde meydana gelebilecek bir saldırıyı saldırı gerçekleşmeden önce tespit eder ve önlem alınmasını sağlar.

8. Siber Güvenlikte İnsan Faktörünün Geleceği

Teknolojiler ne kadar gelişirse gelişsin, insan faktörü siber güvenliğin en önemli unsurlarından biri olmaya devam edecek. Gelecekte, çalışanların siber güvenlik farkındalığını artırmak için daha yenilikçi eğitimler ve simülasyonlar düzenlenecek. Özellikle sosyal mühendislik ve kimlik avı saldırılarına karşı bilinçlendirme programları genişletilecek.

- **Örnek:** Sanal gerçeklik (VR) tabanlı eğitimlerle çalışanlar, olası siber saldırı senaryoları içinde bulunarak bu saldırılara nasıl tepki vereceklerini öğrenir. Bu eğitimler, çalışanların daha güvenli dijital davranışlar sergilemelerine yardımcı olur.

Genel Değerlendirme

Gelecekte siber güvenlik, teknoloji geliştikçe daha karmaşık ve sofistike hale gelen tehditlerle mücadele etmek için sürekli evrilen bir alan olacak. Yapay zeka, kuantum bilgisayarlar, blockchain ve IoT gibi teknolojilerin siber güvenliğe etkileri, hem yeni fırsatlar hem de yeni zorluklar getirecek. İnsan faktörü de bu teknolojilerin yanında siber güvenlikte önemli bir unsur olarak kalmaya devam edecek. Bu nedenle, teknolojik yeniliklere ayak uydurmak ve siber güvenlik stratejilerini sürekli olarak güncellemek, hem bireylerin hem de kurumların güvenliğini sağlamak için kritik öneme sahip olacaktır.

Yapay Zeka ile Siber Güvenlik Uygulamaları

Yapay zeka (AI), siber güvenlik alanında devrim yaratan bir teknolojidir. Geleneksel güvenlik çözümleri, sürekli zorluklarla ve daha karmaşık hale gelen siber tehditlerle başa çıkılamazken, yapay zeka tabanlı uygulamalar daha dinamik ve proaktif bir güvenlik yaklaşımı sunuyor. Yapay zeka, büyük veri analitiği, makine geliştirmei (ML) ve doğal dil işleme (NLP) gibi teknolojik özellikler sistemleri sayesinde tehditleri daha hızlı tespit edebilir, saldırılara karşı otomatik yanıt verebilir ve ortaya çıkan saldırıları tahmin edebilir.

Aşağıda yapay zeka destekli siber güvenlik uygulamaları detaylı bir şekilde ele alınmıştır:

1. Tehdit Tespiti ve Anomali Algılama

Yapay zeka, büyük miktarda veri analiz etme yeteneği sayesinde ağ bağlantısında veya sistemdeki normal olmayan aktiviteleri tespit etmek için kullanılır. AI tabanlı sistemler, makine hesaplamaları ile normal sistem öğrenimini öğrenir ve bu sürecin hedefleri arasında kalan herhangi bir anormalliğin tespiti için sürekli olarak sistemi izler. Bu, siber saldırıların erken aşamalarda tespit edilmesini sağlar.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Bir sağlık sisteminde AI tabanlı güvenlik sistemi, ağ üzerindeki tüm veri takipleri ve normalden sapmalar olduğunda (bunların büyük miktarda veri alışverişi veya beklenen indirimlere girişleri) anında güvenlik ekiplerinin üyeleri. Böylece saldırı gerçekleşmeden önce izleme alınıyor.

2. Otomatik Tehdit Yanıtı ve Müdahale

Yapay zeka, yalnızca tehditleri tespit etmekle kalmaz, aynı zamanda tehditlere karşı otomatik müdahale yeteneği de sunar. Yapay zeka temelli siber güvenlik sistemleri, doğrudan güvenlik politikalarını devreye sokarak zararlı faaliyetleri engelleyebilir. Bu, özellikle siber saldırılar sırasında zaman kayıplarını ve saldırıların maruziyetlerini en aza indirir.

- **Örnek:** Bir yapay zeka destekli güvenlik sistemi, bir fidye yazılım saldırısının çözüldüğü tespit edildiğinde otomatik olarak etkilenen sistemler yayılır ve saldırının ağda çözülmelerini engeller. Ayrıca yapay zeka sistemi olay raporları güvenlik birimlerine detaylı bilgi sunar.

3. Gelişmiş Kötü Amaçlı Yazılım Tespiti

Yapay zeka, özellikle bilinmeyen kötü amaçlı yazılımların (kötü amaçlı yazılım) tespitinde büyük bir rol oynar. Geleneksel antivirüs çözümleri, yalnızca daha önceden tanımlanmış tehditleri tespit edebilirken, AI, kötü amaçlı yazılımların yeni özelliklerini da tanıyabilir. Makine çalıştırmaları, bilinen kötü amaçlı yazılımların davranış kalıplarını analiz eder ve benzer büyüme gösteren yeni tehditleri tespit eder.

- **Örnek:** Bir güvenlik sistemi, AI sayesinde bilinmeyen bir zararlı yazılımın sistemdeki hareketlerini izler ve normal devre dışı hareketleri (bunların, yetkisiz veri şifrelemesi veya sistem kaynaklarının aşırı tüketilmesi) tespit ederek saldırıyı durdurur.

4. Siber Tehdit İstihbaratı

Yapay zeka, siber tehdit istihbaratının etkili bir şekilde büyütülmesine ve analiz edilmesinin daha yararlı olmasına yardımcı olur. Yapay zeka sistemleri, dünya bileşenlerini verileri analiz ederek yeni tehdit trendlerini ve saldırı modellerini öğrenir. Böylece kurumlar, gelecekte karşılaşılabilecek saldırılara karşı proaktif savunma sistemleri geliştirebilir.

- **Örnek:** AI tabanlı tehdit istihbarat sistemleri, dünya genelindeki siber saldırı raporlarını analiz ederek benzer saldırıların yerel ağda ortaya çıkma ihtimali hesaplar. Bu bilgi sayesinde güvenlik ekipleri, saldırı gerçekleşmeden önce gerekli önlemleri alabilir.

5. Kimlik Doğrulama ve Sahtekarlık Tespiti

AI, kimlik süreç süreçlerini daha güvenli hale getirmek için kullanılabilir. Geleneksel parola ve kimlik rejimi yöntemlerinin yetersiz kalması, yapay zeka tabanlı biyometrik sistemler (yüz tanıma, parmak izi, iris tarama vb.) kimlik takibinin doğruluğunu sağlayabilir. Ayrıca AI, sahte kimlik doğrulama girişimlerini anında tespit edebilir ve engelleyebilir.

- **Örnek:** Bir bankada AI tabanlı bir kimlik doğrulama sistemi, kayıtların yüz tanınmaması kullanarak hesaplarına güvenli erişim sağlar. AI, aynı zamanda sahte yüz maskeleri veya kimlik avı girişimlerini tespit edebilir ve bu tür sahte girişleri otomatik olarak engeller.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

6. Kimlik Avı (Kimlik Avı) Saldırılarına Karşı Koruma

Yapay zeka, kimlik avı saldırılarını tespit etmede çok etkilidir. AI, e-postalar ve web siteleri üzerinde yapılan analizler sayesinde sahte veya şüpheli içerikler tespit edilebilir. AI tabanlı sistemler, e-postaları veya web sitelerini inceleyerek, içerikte yer alan tehdit emin olmadıklarını ve sosyal mühendislik tekniklerini hızlı bir şekilde seçerler.

- **Örnek:** AI tabanlı bir e-posta güvenlik sistemi, bir çalışana gelen kimlik avı e-postasını analiz eder ve e-postadaki dil, bağlantıları ve gönderenleri inceleyerek bunu sahte bir e-posta olarak işaretler. Çalışan e-postayı açmadan önce uyarı alır.

7. Verilerin Şifrelenmesi ve Güvenli Veri Aktarımı

AI, veri güvenliği konusunda önemli bir rol oynar. Verilerin şifrelenmesi ve güvenli aktarımı gibi durumlarda yapay zeka, verilerin gizli bir şekilde korunmasını sağlayacak dinamik şifreleme işlemleri geliştirilebilir. Ayrıca, çözme çözümleri üzerindeki güvenlik açıklarını sürekli olarak tespit edip durdurabilir.

- **Örnek:** Yapay zeka destekli bir güvenlik sistemi, bir sağlık sisteminin hasta rejiminin bozulması için her sistemin farklı ve dinamik bir şifreleme sistemi kullanarak veri transferini güvenli hale getirir. Ayrıca, veriler yetkisiz bir kullanıcı tarafından şifrelenmeye çalışıldığında sistemi kilitler.

8. Güvenlik Açıklarının Tespiti (Güvenlik Açığı Taraması)

Yapay zeka, sistemlerdeki güvenlik açıklarını taramak ve bu açıkları insan müdahalesine gerek kalmadan hızlı bir şekilde tespit etmek için kullanılabilir. Yapay zeka sistemi güvenlik açığı tarama sistemleri, yazılım güncellemelerini izler, zayıflıkları analiz eder ve bu açıkları hızlı bir şekilde güvenlik ekiplerine bildirir.

- **Örnek:** AI destekli bir güvenlik sistemi, seçim ağında veya yazılımda bulunan potansiyel güvenlik açıklarını sürekli olarak izliyor ve bu açıkların nasıl kapatılabileceği konusunda önerilerde bulunuyor. Yapay zeka sayesinde bu süreç daha hızlı ve etkin hale gelir.

9. Davranışsal Analiz ve Proaktif Tehdit Tespiti

Yapay zeka, kullanıcıların ve sistemlerin normal davranışlarının kalıplarını öğrenir ve bu kalıpların birleşiminden oluşan faaliyetleri tespit edebilir. Bu tür davranışsal analizler, proaktif tehdit miktarının kapsamı önemlidir. AI, kullanıcıların kapasitelerini analiz ederek, sistem ortaya çıkan olağandışı faaliyetler daha iyi tanınabilir ve olası tehditlere karşı erken uyarı verebilir.

- **Örnek:** Bir çalışanın hesabında olağandışı bir davranış (örneğin, gece boyunca çok sayıda dosya indirilmesi veya farklı bir paylaşımlı giriş yapılması) tespit ayrılıkları, AI bu durumu potansiyel bir tehdit olarak işaretler ve güvenlik ekiplerine uyarı sistemi.

10. Siber Güvenlik Eğitimi ve Farkındalık

Yapay zeka, siber güvenlik eğitimlerinde ve uzaktan programlarda da mevcuttur. Yapay zeka temelli eğitim sistemleri, insanların zayıf noktalarını analiz ederek onlara özel eğitimler sunabilir. Ayrıca simülasyonlar ve sanal gerçeklik düzeyinde eğitim programları, kişilerin gerçek saldırı senaryolarına karşı nasıl tepki vereceklerini öğrenmelerini sağlar.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Bir sağlık sorunu, çalışanlarına yapay zeka destekli siber güvenlik eğitimi vererek, çalışanın zayıf yönlerine göre kişiselleştirilmiş eğitim modülleri sunuyor. Bu sayede onun çalışan, en çok ihtiyaç duyduğu alanlardaki birikimini artırabilir.

Yapay zeka, siber güvenlik dünyasında devrim yaratan bir teknoloji olarak karşımıza çıkıyor. Tehditlerin tespit edilmesi, saldırılara otomatik yanıt verilmesi, bilinmeyen kötü amaçlı yazılımların engellenmesi ve proaktif güvenlik stratejilerinin geliştirilmesi gibi birçok alanda AI tabanlı çözümler etkin bir şekilde kullanılmaktadır. AI, siber güvenlik ekiplerinin iş yükünü azaltırken, sistemlerin güvenliğini artırmak ve olası tehditlere karşı daha güçlü bir savunma hattı oluşturmak için önemli fırsatlar sunmaktadır. Gelecekte yapay zeka destekli siber güvenlik uygulamaları, daha da sofistike hale gelecek ve dijital dünyadaki güvenlik zorluklarına karşı güçlü bir savunma mekanizması sağlayacaktır.

Makine Öğrenmesi Siber Güvenlikte Nasıl Kullanılır?

Makine öğrenmesi (ML), siber güvenlik alanında güçlü bir araç haline getirildi. ML, büyük miktarda veriyi analiz edebilme, yeni tehditleri öğrenme ve anormallik tespit edebilme yeteneğiyle siber güvenlikteki birçok geleneksel yöntem daha etkili hale geliyor. Aşağıda, makine öğrenmesinin siber güvenlikte nasıl faaliyet gösterdiğine dair ayrıntılı bir inceleme yer almaktadır.

1. Anormal Tespiti

Makine öğrenmesi, anormal durumun tespit edilmesinde yaygın olarak kullanılan işlemlerden biridir. Sistemlerde ortaya çıkan olağan dışı etkinlikler, potansiyel bir saldırı belirtisi olabilir. ML modelleri, sistemlerin ve ağların normal öğrendiğini öğrenir ve bu davranıştan sapmaları tespit eder. Bu anormallikler, potansiyel bir saldırının erken belirtisi olabilir ve bu sayede saldı

- **Örnek:** Bir ağ üzerindeki normal bağlantı öğrenen bir makine öğrenmesi modeli, kendisinden artan veri transferlerini veya beklenen saatlerde giriş denemelerini anormallik olarak işaretleyebilir. Bu tespit, bir DDoS saldırısı veya veri sızıntısının erken aşamada fark edilmesini mümkün kılar.

2. Kötü Amaçlı Yazılım Tespiti

Geleneksel antivirüs yazılımları, genellikle kötü amaçlı yazılımları (kötü amaçlı yazılım) bilinen imzalarına göre tespit eder. Ancak makine öğrenmesi, kötü amaçlı yazılımların yeni, henüz tanınmaması

- **Örnek:** Bir makine öğrenmesi modeli, zararlı yazılımların genellikle sistem kaynaklarının aşırı tüketimi, veri şifrelemesi veya beklenen ağ bağlantılarını kurması gibi kalıpları öğrenir. Bu model, daha önce tanımlanmamış bir zararlı yazılımın sisteminin benzer davranışlar sergilemesi durumunda alarm verebilir.

3. Kimlik Avı (Phishing) Saldırılarını Önleme

Makine öğrenmesi, kimlik avı saldırılarını tespit etmek için kullanılabilir. ML yazılımları, e-postalar ve web sitelerindeki metin, dağıtıcı ve kopyalayıcı analiz ederek kimlik avı girişimlerini tanıyabilir. Bu sayede sahte e-postalar ve dolandırıcı web siteleri daha güvenli bir şekilde

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Bir makine öğrenmesi modeli, gelen e-postaların dilini analiz ederek kimlik avı tekniklerini (tehditler, aciliyet oluşturma, şüpheli girişler vb.) tanıyabilir ve bu e-postaları kullanıcılar açmadan önce tehlikeli olarak işaretleyebilir.

4. Davranışsal Analiz ve Kullanıcı Profillemesi

Makinenin öğrenmesi, kullanıcıların normal koşullarındaki değişiklikleri ve bu davranışlardan sapmaları tespit edilebilir. Her kullanıcının bilgisayarında yaşamına ve ağ yapısına dayalı olarak profiller oluşturulabilir. Bu profilleme sayesinde, bir Saldırgan bir kişinin kimliğini edinebileceğinde, kişinin kullanabileceği bir şekilde davranması durumunda anormallik fark edilebilir.

- **Örnek:** Bir çalışan normal çalışma aralıkları belirli dosyalara erişirken, gece geçiş oranları farklı bir cihazdan çok sayıda dosya indirmeye çalışırsa, makine öğrenmesi çalışması bu fark çalışması ve olası bir kırılma olup olmadığını belirlemeir.

5. Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)

Makine öğrenmesi, ağ trafolarındaki sa

- **Örnek:** Bir IDS sistemi, sürekli olarak ağdaki tüm giriş ve çıkış işlemlerini inceler ve makine öğrenmesi sayesinde normal olmayan durumları (örneğin, şüpheli bir IP'den gelen yoğun trafik) tespit eder. Sistem, saldırıyı daha geniş bir veri analizi ile anlamlandırarak saldırı gerçekleşmeden önce müdahale eder.

6. Siber Tehdit İstihbaratı

Makine öğrenmesi, siber tehdit istihbaratında kullanılan büyük veri setlerini analiz etmek için kullanılabilir. Dünya genelindeki tehditlerin analizini yapan ML indirmeleri, yeni ortaya çıkan saldırı yöntemleri ve saldırı kalıplarını belirlendi. Bu da daha proaktif bir siber güvenlik stratejisi geliştirmelerine yardımcı olur.

- **Örnek:** Dünya çapında gerçekleşen siber saldırılar

7. Güvenlik Açığı Yönetimi

Makine öğrenmesi, bir sistemdeki potansiyel güvenlik açıklarını daha hızlı bir şekilde tespit edebilir ve güvenlik ekiplerinin bu açıkları kapatmasına yardımcı olabilir. ML sistem sistemleri, yazılım zafiyetlerini otomatik olarak analiz eder, hangi güvenlik açıklarının en ciddi tehdidin şeffaflığını sağlar ve kişisel önlemler önerir.

- **Örnek:** Bir güvenlik açığı tarama aracı, sistemdeki yer alan yazılımlardaki tüm güvenlik açıklarını analiz eder ve bu açıkların nasıl kapatılacağı konusunda önerilerde bulunur. Makine öğrenmesi, hangi açıkların daha kritik olduğunu belirleyerek güvenlik ekiplerinin zamanlarını daha verimli kullanmasını sağlar.

8. Otomatik Yanıt Sistemleri

Makine öğrenmesi, siber saldırılara otomatik olarak yanıt veren kapsamlı içeriklerde kullanılır. ML tabanlı otomatik yanıt sistemleri, tehdit değişimi güvenlik politikalarını devreye sokarak zararlı hizmetler sistemlerine zarar vermesini önleyebilir. Bu sistemleri, tehditleri izole edebilir, zararlı yazılımları temizleyebilir veya şüpheli kullanıcılar sistemden çıkarabilir gibi işlemleri otomatik olarak yapabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Bir otomatik yanıt sistemi, fidye yazılım saldırısı tespitleri, anlık etkilenen sistemleri dağıtır, saldırının geri kalana ayrılmasını engeller ve güvenlik ekiplerine saldırı raporları sunar.

9. Sosyal Mühendislik Saldırılarına Karşı Koruma

Sosyal mühendislik saldırıları, insan faktörüne dayalı siber saldırılardır ve geleneksel güvenlik önlemlerinden kaçabilir. Ancak makine öğrenmesi, sosyal mühendislik saldırılarını tespit etmekte etkili olabilir. Bu tür saldırılarda kullanılan teknikler, dil işleme ve davranış analizi gibi erişimler öğrenilebilir ve bu sayede bu saldırılara karşı daha etkili koruma bölünmesi.

- **Örnek:** Bir şirketin makine öğrenmesi sistemi, kişilerin günlük e-posta yazışmalarını ve mesajlaşmalarını analiz eder. Sistem, sosyal mühendislik teknikleri içeren şüpheli mesajları tespit ederek üyelerini birleştirir.

Makine öğrenmesi, siber güvenlik tehditlerinin daha etkili ve proaktif bir şekilde tespit edilmesi ve önlenmesi için güçlü bir teknoloji haline getirildi. Anomali farklılıkları, kötü amaçlı yazılımların ayrılması, kimlik avı saldırılarının önlenmesi, güvenlik açıklarının yönetimi ve otomatik yanıt sistemleri gibi birçok alanda makine öğrenmesi, geleneksel güvenlik yöntemleriyle karşılaştırma çok daha hızlı ve esneklik sağlar.

Yapay zeka bir strateji belirleyebilir mi?

1. IoT Ağlarında Anomali Tespiti

Yapay zeka algoritmaları, IoT cihazlarının ve ağlarının normal davranışlarını öğrenebilir

- **Örnek:** Akıllı bir

2. Gerçek zamanlı tehdit algılama ve yanıtlama

Nesnelerin İnterneti cihazları genellikle iletişim açısından kısıtlıdır

- **Örnek:** Bir üretim tesisinde

3. AI tabanlı Cihaz Kimlik Doğrulaması ve Erişim Kontrolü

Yapay zeka, m'yi analiz ederek IoT cihazı kimlik doğrulamasını iyileştirebilir

- **Örnek:** AI tabanlı erişim kontrolü şu şekilde uygulanabilir:

4. IoT Cihazları için Tahmini Bakım

Yapay zeka tespit etmeye yardımcı olabilir

- **Örnek:** Yapay zeka, IoT tabanlı akıllı bir cihazı izliyor

5. Otomatik Ürün Yazılımı Güncellemeleri ve Yama Uygulamaları

En büyük güvenlik zorluklarından biri

- **Örnek:** Akıllı bir şehirde, AI-

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

6. Cihaz Bütünlüğü için Davranışsal Profilleme

Yapay zeka ayrıntılı davranışsal profiller oluşturabilir

- **Örnek:** Bağlı bir güvenlik kamerası genellikle günün belirli saatlerinde düşük bant genişliğine sahip video akışları gönderir. Yapay zeka, kameranın alışılmadık bir zamanda aniden büyük miktarda veri ilettiğini tespit ederse, bu yetkisiz uzaktan görüntüleme veya veri sızdırma gibi bir siber saldırının göstergesi olabilir.

7. Dağıtılmış Hizmet Reddi (DDoS) Saldırılarının Önlenmesi

IoT cihazları genellikle botnet'lere dahil edilir ve zayıf güvenlik yapılandırmaları nedeniyle büyük ölçekli Dağıtılmış Hizmet Reddi (DDoS) saldırıları için kullanılır. Yapay zeka, cihazların anormal trafik oluşturmak için kullanıldığı veya bilinen botnet komuta ve kontrol sunucularıyla iletişim kurduğu zamanları belirleyerek botnet katılımının işaretlerini tespit edebilir.

- **Örnek:** IoT özellikli akıllı cihazların ağını izleyen AI sistemleri, belirli cihazların DDoS saldırısıyla tutarlı trafik kalıpları ürettiğini tespit eder. Sistem bu cihazları tehlikeye atılmış olarak işaretler ve saldırıya katılmalarını önlemek için ağdan kaldırır.

8. IoT Edge Cihazlarının Güvenliğini Sağlama

Verilerin işlendiği uç bilişim

- **Örnek:** Hasta verilerinin gerçek zamanlı analiz için uçta işlendiği bir sağlık hizmeti IoT sisteminde, yapay zeka algoritmaları yalnızca kimliği doğrulanmış cihazların hassas verilere erişmesini sağlayabilir ve verileri sızdırma girişimlerini izleyebilir.

9. Akıllı Trafik Yönlendirme ve Yük Dengeleme

Yapay zeka, ağ trafiğini analiz ederek ve verilerin cihazlar arasında nasıl aktığını dinamik olarak ayarlayarak IoT cihaz iletişiminin verimliliğini ve güvenliğini artırabilir. Yapay zeka, olası darboğazları belirleyebilir, trafiği savunmasız yollardan kaçınmak için yeniden yönlendirebilir ve verilerin aktarım sırasında şifrelenmesini sağlayabilir.

- **Örnek:** Bağlantılı bir araç sisteminde, yapay zeka otonom araçlar arasındaki trafiği analiz edebilir ve ağda herhangi bir güvenlik açığı tespit edilirse iletişimi güvenli yollar üzerinden yeniden yönlendirebilir, böylece yolcuların güvenliğini ve aracın verilerinin bütünlüğünü sağlayabilir.

10. AI destekli şifreleme ve güvenli iletişim

Yapay zeka, gerçek zamanlı veri analizine dayalı daha uyarlanabilir şifreleme modelleri geliştirerek geleneksel şifreleme yöntemlerini iyileştirebilir. Sınırlı işlem gücüne sahip IoT cihazları için yapay zeka, geliştirmeden ödün vermeden sağlam güvenlik sağlamak için şifreleme algoritmalarını optimize etmeye yardımcı olabilir.

- **Örnek:** Akıllı ev ortamındaki yapay zeka sistemleri, iletilen verilerin hassasiyetine bağlı olarak şifreleme seviyelerini dinamik olarak ayarlayabilir ve böylece akıllı termostatlar veya sensörler gibi düşük güç tüketen cihazlarda bile güvenliğin sağlanmasını garanti altına alabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

Çözüm

Yapay zeka, gerçek zamanlı tehdit tespiti sağlayarak, güvenlik açığı yönetimini otomatikleştirerek ve iletişim ve kimlik doğrulama süreçlerini optimize ederek IoT cihazlarının güvenliğini büyük ölçüde artırabilir. IoT cihazlarının sayısı artmaya devam ettikçe, AI'nın bu cihazları gelişen siber tehditlerden korumadaki rolü daha da önemli hale gelecektir. AI destekli güvenlik çözümleriyle IoT ağları saldırılara karşı daha iyi korunabilir ve hem operasyonel verimlilik hem de veri bütünlüğü sağlanabilir.

Yaygın loT Güvenlik Riskleri Nelerdir?

1. Zayıf veya Sabit Kodlu Parolalar

Birçok IoT cihazı, varsayılan veya sabit kodlanmış parolalarla birlikte gelir; bu parolalar

- **Örnek:** Varsayılan yönetici parolasına sahip akıllı bir kamera hacklenebilir ve

2. Düzenli Yazılım Güncellemeleri ve Yamalarının Eksikliği

IoT cihazları genellikle bilinen güvenlik açıklarına sahip güncel olmayan yazılımlar çalıştırır. Üreticiler bazen düzenli ürün yazılımı güncellemeleri sağlamaz veya kullanıcılar bunları uygulamayı ihmal eder ve bu da cihazları bilinen istismarlara karşı savunmasız bırakır.

- **Örnek:** Akıllı

3. Güvensiz İletişim Protokolleri

Birçok IoT cihazı güvenli olmayan ağlar üzerinden iletişim kurar

- **Örnek:** Akıllı bir ev cihazı ağ üzerinden düz metin (şifrelenmemiş) olarak veri gönderirse, bir saldırgan hassas bilgileri yakalayabilir ve okuyabilir.

4. Yetersiz Veri Şifrelemesi

Depoladıkları veya ilettikleri verileri düzgün bir şekilde şifrelemeyen IoT cihazları,

- **Örnek:** Kullanıcının sağlık verilerini şifrelemeden saklayan bir fitness takip cihazı şu şekilde olabilir:

5. Cihaz Kaçırma

Saldırganlar kontrolü ele geçirebilir

- **Örnek:** Bir bilgisayar korsanı akıllı ev kameralarını ele geçirip bunları ev sahiplerini gözetlemek için kullanabilir veya bunları web sitelerine büyük ölçekli DDoS saldırıları başlatmak için bir botnetin parçası haline getirebilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

6. Botnet Saldırıları

Nesnelerin İnterneti (IoT) cihazları, insan kaynakları için birincil hedeflerdir

- **Örnek:** Mirai **botnet'i** , en yaygın olanlardan biridir.

7. Fiziksel Güvenlik Riskleri

Özellikle kamuya açık alanlarda kullanılan IoT cihazları

- **Örnek:** Bir evin dışına kurulan akıllı kilit

8. Güvenli Olmayan Web Arayüzleri

Birçok IoT

- **Örnek:** Zayıf güvenlikli bir web kullanan akıllı bir aydınlatma sistemi

9. Zayıf Kimlik ve Erişim Yönetimi

IoT cihazları

- **Örnek:** Bir iyileşme

10. Kötü Amaçlı Yazılımlara Karşı Güvenlik Açığı

IoT cihazı

- **Örnek:** IoT kötü amaçlı yazılımı gibi**"BrickerBot"** cihazlara bulaşabilir ve depolama ve yapılandırma ayarlarını bozarak kullanılmaz hale getirebilir, yani cihazı "tuğlalaştırabilir".

11. Zayıf Güvenlikli API'ler (Uygulama Programlama Arayüzleri)

API'ler genellikle IoT cihazları tarafından diğer cihazlarla veya bulut hizmetleriyle etkileşim kurmak için kullanılır

- **Örnek:** Bir

12. Gizlilik Endişeleri

Birçok IoT cihazı büyük miktarda hassas veri toplar

- **Örnek:** Sürekli olarak l

13. Sınırlı İşlem Gücü ve Güvenlik Yetenekleri

IoT cihazları genellikle sınırlı işlem gücüne ve belleğe sahiptir ve bu da güçlü şifreleme, güvenlik protokolleri veya düzenli güvenlik güncellemeleri uygulamayı zorlaştırır. Bu onları daha savunmasız bırakır

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Endüstriyel bir kontrol sisteminde kullanılan küçük bir IoT sensörü, sofistike bir IoT sensörünü çalıştırmak için gereken işlem gücüne sahip olmayabilir.

14. Tedarik Zinciri Güvenlik Açıkları

IoT cihazları genellikle çeşitli satıcılardan alınan bileşenlere veya yazılımlara sahiptir. Tedarik zincirinin herhangi bir parçası comp

- **Örnek:** Güvenli olmayan bir üçüncü taraf çipi kullanan bir IoT aygıtı, saldırganların güvenlik önlemlerini atlatmak için yararlanabileceği bir donanım arka kapısına sahip olabilir

15. Yetersiz Güvenlik Yapılandırmaları

Birçok IoT cihazı zayıf varsayılan ayarlarla veya varsayılan olarak etkinleştirilmiş güvenlik yapılandırmaları olmadan gönderilir. Kullanıcılar bu cihazları yapılandırma ihtiyacının farkında olmayabilir

- **Örnek:** Akıllı bir termostat şunları sağlayabilir:

Çözüm

IoT geliştirme

Siber güvenlikte yapay zekanın örnekleri nelerdir?

Yapay zeka, siber tehditleri tespit etmek, önlemek ve bunlara yanıt vermek için gelişmiş çözümler sunarak siber güvenlikte giderek daha kritik bir rol oynamaktadır. Aşağıda yapay zekanın siber güvenlikte nasıl kullanıldığına dair bazı temel örnekler verilmiştir:

1. AI Destekli Tehdit Algılama

Yapay zeka sistemleri, büyük miktarda veriyi analiz edebilir ve kötü amaçlı aktiviteye işaret edebilecek kalıpları belirleyebilir. Bu sistemler, önceki saldırılardan sürekli olarak ders çıkarır ve yerleşik kalıplardan sapan anormallikleri veya şüpheli davranışları belirleyerek yeni tehditleri tespit edebilir.

- **Örnek: Darktrace,** yapay zekayı kullanarak ağ trafiğini gerçek zamanlı olarak izler ve belirli bir ağ için normal davranışın ne olduğunu öğrenir. İçeriden gelen bir tehdit, kötü amaçlı yazılım veya veri ihlalini gösterebilecek olağandışı bir etkinlik tespit ettiğinde, güvenlik ekiplerini uyarır ve tehdidi azaltmak için otomatik adımlar atar.

2. Davranış Analizi ve Anomali Tespiti

Yapay zeka, kullanıcılar, cihazlar ve sistemler için normal davranış profilleri oluşturabilir. Yapay zeka, bu profilleri sürekli analiz ederek, bir siber saldırıyı gösterebilecek anormal davranışları tespit edebilir. Bu, özellikle içeriden gelen tehditleri, kimlik avı saldırılarını ve diğer gizli saldırı biçimlerini tespit etmek için faydalıdır.

- **Örnek: Exabeam,** içeriden gelen tehditleri tespit etmek için kullanıcı ve varlık davranışı analitiği (UEBA) için AI kullanır. Normal kullanıcı davranışını izler ve hassas dosyalara tuhaf saatlerde erişim veya alışılmadık bir konumdan oturum açma gibi olağan dışı etkinlikleri işaretler.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

3. AI Destekli Güvenlik Bilgi ve Olay Yönetimi (SIEM)

Yapay zeka, çeşitli kaynaklardan gelen verilerin korelasyonunu iyileştirerek, tehditlerin tespitini otomatikleştirerek ve yanlış pozitifleri azaltarak geleneksel SIEM sistemlerini geliştirir. Makine öğrenimi modelleri, manuel kural belirlemeye gerek kalmadan verilerden otomatik olarak öğrenebilir ve yeni tehditlere uyum sağlayabilir.

- **Örnek: IBM QRadar,** çeşitli kaynaklardan (günlükler, ağ akışları, olaylar) gelen verileri ilişkilendirmek ve analiz etmek ve araştırma için en kritik güvenlik olaylarına öncelik vermek için yapay zekayı kullanır. Bu, tespit ve yanıt sürecini hızlandırır ve tespit ile azaltma arasındaki süreyi azaltır.

4. Kötü Amaçlı Yazılım Algılama ve Önleme

Yapay zeka modelleri, imzalar yerine davranışa göre kötü amaçlı yazılımları tespit edebilir, bu da daha önce bilinmeyen kötü amaçlı yazılım çeşitlerini tespit edebilecekleri anlamına gelir. Makine öğrenimi algoritmaları, bilinen kötü amaçlı yazılımların belirli imzalarını aramak yerine programların nasıl davrandığını analiz eder ve bu da bilgisayar korsanlarının tespitten kaçmasını zorlaştırır.

- **Örnek: Cylance,** milyonlarca dosya özniteliğini analiz ederek ve kötü amaçlı davranış kalıplarını belirleyerek kötü amaçlı yazılımları yürütmeden önce tespit etmek ve engellemek için yapay zekayı kullanır. Geleneksel imza tabanlı sistemlerin gözden kaçırabileceği sıfırıncı gün tehditlerini ve polimorfik kötü amaçlı yazılımları tespit edebilir.

5. Otomatik Olay Yanıtlama

Yapay zeka, tehditlerin tanımlanmasını ve düzeltilmesini otomatikleştirerek olay müdahalesine yardımcı olabilir. Bu, müdahale süresini azaltır ve saldırıların yayılmasını önlemeye yardımcı olur. Yapay zeka sistemleri, enfekte cihazları izole etme, şüpheli trafiği engelleme veya tehlikeye atılmış kullanıcı kimlik bilgilerini sıfırlama gibi önceden tanımlanmış eylemler gerçekleştirebilir.

- **Örnek:** **F**FireEye Helix,** AI'yı olay müdahalesiyle bütünleştirir, tehditleri gerçek zamanlı olarak otomatik olarak sınırlandırır ve azaltır. Örneğin, tehlikeye atılmış bir cihaz tespit ettiğinde, kötü amaçlı yazılımın yayılmasını önlemek için cihazı ağdan otomatik olarak izole edebilir.

6. Kimlik Avı Tespiti

Yapay zeka, kimlik avı girişimlerini tespit etmek için büyük miktarda e-posta ve web sitesi verisini analiz edebilir. Makine öğrenimi modelleri, alan adlarındaki ufak değişiklikler, şüpheli bağlantılar ve alışılmadık dil kalıpları gibi insan kullanıcıların gözden kaçırabileceği kimlik avının ince göstergelerini belirleyebilir.

- **Örnek: Cofense,** e-posta içeriğini, gönderici davranışını ve meta verileri analiz ederek kimlik avı e-postalarını tespit etmek için AI kullanır. Algılama doğruluğunu iyileştirmek ve gelecekteki kimlik avı girişimlerini işaretlemek için kullanıcılar tarafından bildirilen kimlik avı e-postalarından sürekli olarak öğrenir.

7. Tahmini Tehdit İstihbaratı

Yapay zeka, önceki saldırılardan, mevcut güvenlik açıklarından ve küresel tehdit istihbaratından gelen verileri analiz ederek ortaya çıkan siber tehditleri tahmin edebilir. Tahmine dayalı modeller, altyapılarının hangi

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

alanlarının en savunmasız olduğunu belirleyerek kuruluşların yaklaşan saldırılara hazırlanmasına yardımcı olabilir.

- **Örnek: Recorded Future,** tehdit istihbaratı beslemeleri, geçmiş saldırı verileri ve gerçek zamanlı bilgilerin bir kombinasyonuna dayalı olarak potansiyel siber tehditleri analiz etmek ve tahmin etmek için AI kullanır. AI modelleri, hangi güvenlik açıklarının yakında istismar edilmesinin muhtemel olduğunu tahmin edebilir ve kuruluşların bunları proaktif olarak ele almasına olanak tanır.

8. Finansal Sistemlerde Dolandırıcılık Tespiti

Yapay zeka, kullanıcı işlemlerini analiz ederek ve normdan sapan kalıpları belirleyerek dolandırıcılık faaliyetlerini tespit etmek için kullanılabilir. Bu yaklaşım, dolandırıcılığı, hesap devralmalarını ve kara para aklamayı önlemek için bankacılık ve finansal hizmetlerde yaygın olarak kullanılır.

- **Örnek: PayPal,** kullanıcı davranışından ve işlemlerden binlerce veri noktasını analiz ederek sahtekarlık işlemlerini tespit etmek için yapay zekayı kullanır.

9. AI Tabanlı Kimlik ve Erişim Yönetimi

Yapay zeka, yetkisiz erişimi tespit etmek için kullanıcı davranışını analiz ederek kimlik ve erişim yönetimini iyileştirebilir. Tehlikeye atılmış bir hesabı gösterebilecek alışılmadık oturum açma konumlarını, zamanlarını veya kalıplarını belirleyebilir ve çok faktörlü kimlik doğrulamayı (MFA) otomatik olarak tetikleyebilir veya erişimi tamamen engelleyebilir.

- **Örnek: Okta,** oturum açma girişimleri sırasında riski sürekli olarak değerlendirmek için AI'yı kimlik yönetimi platformuna entegre eder. AI, bir kullanıcının oturum açma davranışının alışılmadık olduğunu, örneğin yeni bir ülkeden oturum açtığını tespit ederse, ek doğrulama adımlarını tetikleyebilir veya kullanıcının kimliği doğrulanana kadar erişimi engelleyebilir.

10. AI-Geliştirilmiş Penetrasyon Testi

Yapay zeka, bir sistemdeki güvenlik açıklarını bulma sürecini otomatikleştirerek penetrasyon testine yardımcı olabilir. Yapay zeka destekli penetrasyon testi araçları, sistemleri zayıflıklar açısından sürekli olarak test edebilir ve analiz edebilir ve güvenlik ekiplerine güvenlik duruşlarının dinamik bir görünümünü sağlayabilir.

- **Örnek: Synack,** sızma testi sürecinin bazı kısımlarını otomatikleştirerek insan etik hacker'larını desteklemek için AI kullanır. AI, potansiyel güvenlik açıklarını daha hızlı tespit etmeye yardımcı olur ve insan testçilerin bu zayıflıkları doğrulamaya ve kullanmaya odaklanmasını sağlar.

11. Ağ Trafiği İzleme

Yapay zeka tabanlı araçlar, olağandışı veri aktarım hızları, yetkisiz erişim girişimleri veya ağa bağlanan bilinmeyen cihazlar gibi şüpheli etkinlikleri tespit etmek için ağ trafiğini gerçek zamanlı olarak izleyebilir. Yapay zeka modelleri normal ağ davranışını öğrenir ve daha fazla araştırma için sapmaları işaretler.

- **Örnek: Vectra,** dahili ağ trafiğini izlemek ve ağ içindeki yanal hareket veya tehlikeye atılmış cihazlardan gelen komuta ve kontrol iletişimi gibi gerçek zamanlı siber saldırıları tespit etmek için yapay zekayı kullanır. Kuruluşların geleneksel güvenlik duvarlarının veya kötü amaçlı yazılım önleme araçlarının kaçırabileceği tehditleri tespit etmesine yardımcı olur.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

12. Sıfır Gün Saldırısı Algılama

Yapay zeka, yazılım davranışını analiz ederek ve bir istismarı gösterebilecek anormal aktiviteleri tanıyarak sıfırıncı gün zafiyetlerini (önceden bilinmeyen güvenlik açıklarını) belirlemeye yardımcı olabilir. Bu yetenek, kuruluşların henüz bilinen imzaları veya yamaları olmayan yeni tehditleri tespit etmesine olanak tanır.

- **Örnek: Sophos Intercept X,** uygulamaların davranışlarını gerçek zamanlı olarak analiz ederek sıfırıncı gün istismarlarını tespit etmek ve önlemek için derin öğrenmeyi kullanır. Bir güvenlik açığı bilinmese bile, yapay zeka taklit eden etkinlikleri işaretleyebilir ve engelleyebilir

Çözüm

Siber güvenlikteki yapay zeka, geleneksel güvenlik araçlarını geliştirir ve siber tehditlere karşı daha hızlı, daha verimli tespit, önleme ve yanıt sağlar. Büyük miktarda veriyi işleme, önceki saldırılardan ders çıkarma ve yeni saldırı kalıplarına uyum sağlama yeteneği, onu modern güvenlik altyapıları için önemli bir araç haline getirir. Siber tehditler geliştikçe, yapay zekanın siber güvenlikteki rolü büyümeye devam edecek ve kuruluşların giderek daha karmaşık siber saldırıların önünde kalmasına yardımcı olacaktır.

Yapay zeka şifrelenmiş verileri nasıl işler?

Şifrelenmiş verileri işlemek, bilgilere yetkisiz erişimi engellemek için tasarlanmış şifrelemenin doğası nedeniyle AI sistemleri için önemli zorluklar sunar. Şifrelenmiş verilerin doğru şifre çözme anahtarları olmadan okunamayacak şekilde tasarlanması nedeniyle AI sistemleri genellikle şifrelenmiş verileri ham haliyle analiz edemez veya işleyemez. Ancak AI, birkaç dolaylı yöntemle şifrelenmiş veri senaryolarında yine de rol oynayabilir:

1. Şifrelenmiş Trafik İzleme

Yapay zeka, paket boyutları, zamanlama ve akış desenleri gibi meta verilere odaklanarak şifrelenmiş ağ trafiğini şifresini çözmeden izleyebilir ve analiz edebilir. İçeriğe erişim olmasa bile yapay zeka, kötü amaçlı yazılım iletişimi veya veri sızdırma girişimleri gibi kötü amaçlı aktiviteyi gösterebilecek olağandışı davranışları veya anormallikleri tespit edebilir.

- **Örnek:** Bir AI sistemi, belirli bir cihazdan gelen giden bağlantılarda ani bir artış gibi anormal örüntüler için şifrelenmiş HTTPS trafiğini izleyebilir. Bu, iletişimin gerçek içeriği şifrelenmiş olsa bile, kötü amaçlı yazılımın bir komuta ve kontrol sunucusuyla iletişim kurmaya çalıştığını gösterebilir.

2. Şifrelenmiş Veri Akışlarında Anomali Tespiti

Yapay zeka, şifrelenmiş veri akışındaki anormal veri hacimleri, beklenmeyen hedefler veya alışılmadık aktarım zamanlaması gibi anormallikleri tespit etmek için makine öğrenimi modellerini kullanabilir. Bu, olası ihlalleri veya yetkisiz veri sızdırmalarını tespit etmeye yardımcı olabilir.

- **Örnek:** Bir kurumsal ağda, yapay zeka, normalde düşük trafiğe sahip şifreli bir kanalın, alışılmadık saatlerde aniden büyük miktarda veri aktarımı yaşadığını tespit edebilir; bu, veriler şifrelenmiş olsa bile, bir veri ihlali veya içeriden gelen bir tehdit belirtisi olabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

3. Güvenli AI İşleme için Homomorfik Şifreleme

Homomorfik şifreleme, AI modellerinin şifrelenmiş veriler üzerinde şifresini çözmeye gerek kalmadan hesaplamalar yapmasına olanak tanır. Bu tür şifreleme, şifrelenmiş değerler arasındaki matematiksel ilişkileri koruyarak AI'nın sınıflandırma, eğitim veya analiz gibi görevleri yerine getirirken verileri güvenli ve gizli tutmasını sağlar. Bu hesaplamaların sonuçları da şifrelenir, bu nedenle AI asla doğrudan ham verilerle etkileşime girmez.

- **Örnek:** Tıbbi bir araştırma projesinde, hassas hasta verileri gizlilik için şifrelenir, ancak homomorfik şifreleme, bir yapay zeka modelinin bu verileri işlemesine ve altta yatan hasta bilgilerini ifşa etmeden içgörüler (örneğin, hastalık tahmini veya anormallik tespiti) üretmesine olanak tanır.

4. Federasyonlu Öğrenme

Federasyonlu öğrenmede, AI modelleri yerel, şifrelenmiş verileri tutan birden fazla merkezi olmayan cihaz veya sunucuda eğitilir. Ham verileri merkezi bir sunucuya göndermek yerine, yalnızca modelin öğrenilen parametreleri paylaşılır. Bu, AI sistemlerinin doğrudan erişmeden veya şifresini çözmeden verilerden öğrenmesini sağlar.

- **Örnek:** Bir akıllı telefon şirketi, kullanıcıların yerel, şifrelenmiş metin verileri üzerinde modeller eğiterek AI destekli klavye tahminlerini geliştirmek için federasyonlu öğrenmeyi kullanır. Merkezi model, bireysel kullanıcıların hassas bilgilerini ifşa etmeden yerel cihazlardan elde edilen içgörülerle güncellenir.

5. AI Destekli Şifreleme Anahtarı Yönetimi

Yapay zeka, anahtarların güvenli bir şekilde saklanmasını, döndürülmesini ve dağıtılmasını sağlayarak şifreleme anahtarı yönetimini iyileştirmeye yardımcı olabilir. Yapay zeka sistemleri, anahtar erişimindeki anormallikleri tespit edebilir, anahtarların oluşturulmasını ve döndürülmesini otomatikleştirebilir ve bir tehlikeye işaret edebilecek olası anahtar kötüye kullanımını tespit edebilir.

- **Örnek:** Bulut tabanlı bir hizmette, AI şifreleme anahtarlarına erişimi izleyebilir ve anahtarları almaya veya kötüye kullanmaya yönelik yetkisiz girişimleri gösterebilecek olağandışı erişim kalıplarını tespit edebilir. Bir ihlal tespit edilirse, AI otomatik anahtar rotasyonunu tetikleyebilir veya tehlikeye atılmış anahtarlara erişimi iptal edebilir.

6. Post-Kuantum Kriptografisi

Kuantum bilgisayarlar ortaya çıktıkça, potansiyel olarak birçok mevcut şifreleme yöntemini kıracaklardır. Yapay zeka, kuantum hesaplama saldırılarına dirençli olan kuantum sonrası kriptografi algoritmalarının geliştirilmesine ve optimize edilmesine yardımcı olabilir. Yapay zeka, farklı kriptografik yöntemleri analiz edebilir ve performanslarını ve güvenliklerini değerlendirebilir.

- **Örnek:** Yapay zeka, araştırmacıların farklı saldırı senaryolarını simüle ederek ve bu algoritmaların verimliliğini artırarak, büyük ölçekli şifreli iletişimlerde kullanım için pratik olmalarını sağlayarak kuantum dirençli algoritmaların gücünü değerlendirmelerine yardımcı olabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

7. Adli Soruşturmalarda AI Tabanlı Şifre Çözme Yardımı

Belirli yasal veya adli bağlamlarda, AI güvenlik profesyonellerinin verileri şifresini çözmeye veya şifrelenmiş veri akışlarını analiz etmeye çalışmasına yardımcı olabilir. Bu genellikle kısmi şifre çözme anahtarlarına erişim, şifreleme algoritmasındaki zayıflıklar veya şifrelenmiş trafikteki kalıpları analiz ederek yapılır. AI'nın buradaki rolü genellikle hızlandırmaktır

- **Örnek:** Siber güvenlik adli soruşturmasında, yapay zeka araçları, güncel olmayan şifreleme yöntemlerindeki zayıflıkları belirlemeye yardımcı olabilir veya yasal bir soruşturmanın parçası olan şifrelenmiş dosyalarda kaba kuvvetle şifre çözme girişimlerini otomatikleştirebilir.

8. Veri Maskeleme ve Farklı Gizlilik

Yapay zeka, veri maskeleme veya farklı gizlilik gibi teknikleri uygulayarak gizliliği ve güvenliği yönetmeye yardımcı olabilir ve sistemlerin hassas bilgileri ifşa etmeden verilerden öğrenmesini sağlar. Bu yöntemler, yapay zekanın yararlı hesaplamalar yapmasına olanak tanırken bir veri kümesindeki belirli ayrıntıları gizler.

- **Örnek:** Bir sağlık hizmeti ortamında, bir yapay zeka sistemi, araştırmacıların şifrelenmiş verilerdeki eğilimleri ve kalıpları, bireysel hasta bilgilerini ifşa etmeden analiz etmelerine olanak tanırken, hastaların sağlık kayıtlarını anonimleştirmek için farklı gizlilik kullanabilir.

Yapay Zeka ve Şifrelenmiş Veriler İçin Temel Zorluklar

Yapay zekanın şifrelenmiş verileri dolaylı yoldan işlemek için çeşitli yöntemleri olmasına rağmen, dikkate değer zorluklar ve sınırlamalar da bulunmaktadır:

- **Veri Erişilebilirliği:** Yapay zeka sistemleri, kaynak yoğun ve daha yavaş olabilen homomorfik şifreleme veya diğer gelişmiş yöntemler kullanılmadığı sürece şifrelenmiş verilerden doğrudan öğrenemez veya bunları işleyemez.
- **Hesaplama Yükü:** Homomorfik şifreleme gibi teknikler önemli miktarda hesaplama yükü oluşturarak büyük veri kümeleri için gerçek zamanlı işlemeyi zorlaştırır.
- **Gizliliği Koruyan Yapay Zeka:** Veri gizliliğine duyulan ihtiyaç ile yapay zekanın yararlı içgörüler üretme becerisi arasında denge kurmak, özellikle son derece hassas veya düzenlenmiş veriler söz konusu olduğunda hâlâ bir zorluk olmaya devam ediyor.
- **Yasal ve Etik Endişeler:** Şifrelemeyi kırmak veya şifrelenmiş verilere yetkisiz yollarla erişmeye çalışmak için AI kullanımına ilişkin yasal ve etik endişeler vardır. Örneğin, adli şifre çözme oldukça sıkı bir şekilde düzenlenir ve katı yasal protokolleri takip etmelidir.

Çözüm

Yapay zeka, anormallik tespiti, homomorfik şifreleme, federasyonlu öğrenme ve güvenli şifreleme anahtarı yönetimi yoluyla şifrelenmiş verilerin güvenliğini ve yönetimini artırabilir. Ancak yapay zeka, ek hesaplama karmaşıklığı getiren karmaşık şifreleme şemaları olmadan şifrelenmiş verileri doğrudan işleyemez. Şifreleme ve veri gizliliği gereksinimleri geliştikçe yapay zeka, verilerin hem

Evet, AI, diferansiyel gizlilik, birleşik öğrenme, homomorfik şifreleme ve otomatik gizlilik koruma algoritmaları gibi gelişmiş teknikleri kullanarak şifrelemenin yanı sıra veri gizliliğini önemli ölçüde iyileştirebilir. Bu teknolojiler, AI'nın hassas bilgileri ifşa etme riskini en aza indirirken veya ortadan kaldırırken

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

verileri işlemesine ve bunlardan öğrenmesine olanak tanır. Aşağıda AI'nın şifrelemenin yanı sıra veri gizliliğini artırabileceği bazı temel yollar verilmiştir:

1. Farklı Gizlilik

Farklı gizlilik, AI modellerinin bireysel gizliliği sağlamak için verilere kontrollü gürültü eklerken veri kümeleri üzerinde eğitildiği bir tekniktir. Bu, belirli veri noktalarını ortaya çıkarmadan veya veri kümesindeki bireyleri tanımlamadan yararlı içgörülerin çıkarılmasını sağlar. Farklı gizlilik, bir AI modelinin çıktısının eğitimde belirli bir bireyin verilerinin kullanılıp kullanılmadığını ortaya çıkarmamasını sağlar.

- **Örnek:** Bir sağlık hizmeti ortamında, hasta verileri üzerinde eğitilen bir AI modeli, özel hasta bilgilerini ifşa etmeden hastalıklar hakkında tahminler veya içgörüler sağlayabilir. Farklı gizlilik, AI modeli birden fazla kez sorgulansa bile, herhangi bir hasta hakkında belirli ayrıntıları ifşa etmeyeceğinden emin olur.

2. Federasyonlu Öğrenme

Federasyonlu öğrenme, AI modellerinin her biri kendi yerel verilerini tutan birden fazla merkezi olmayan cihaz veya sunucuda eğitilmesine olanak tanır. Ham verileri merkezi bir sunucuya göndermek yerine, yalnızca model güncellemeleri (öğrenilen desenler) paylaşılır ve yerel verilerin gizliliği korunur. Bu yaklaşım, hassas verilerin iletim veya depolama sırasında açığa çıkma veya tehlikeye girme riskini önemli ölçüde azaltır.

- **Örnek:** Bir cep telefonu şirketi

3. Homomorfik Şifreleme

Homomorfik şifreleme, AI algoritmalarının şifrelenmiş veriler üzerinde, önce şifresini çözmeye gerek kalmadan hesaplamalar yapmasına olanak tanır. Bu, tüm hesaplama süreci boyunca verilerin gizliliğini korur ve hassas işlemlerin bile güvenli bir şekilde gerçekleştirilebilmesini sağlar. Homomorfik şifreleme, verilerin hem depolama sırasında hem de işlenirken gizli kalmasını sağlar.

- **Örnek:** Bir finansal hizmetler şirketinde, homomorfik şifreleme, AI modellerinin şifrelenmiş müşteri işlem verilerini analiz ederek gerçek işlem ayrıntılarını ifşa etmeden potansiyel dolandırıcılığı tespit etmesine olanak tanıyabilir. Analizin şifrelenmiş sonuçları daha sonra sisteme geri gönderilir ve bu da tam gizlilik sağlar.

4. Gizliliği Koruyan Makine Öğrenmesi (PPML)

Gizliliği koruyan makine öğrenimi, AI modellerinin ve algoritmalarının kullanıcı gizliliğine saygı göstermesini sağlamaya odaklanır. Güvenli çok taraflı hesaplama (SMPC), şifreleme tabanlı yöntemler ve farklı gizlilik gibi teknikler, verilerin AI eğitimi ve çıkarım süreçleri boyunca korunmasını sağlamak için makine öğrenimi iş akışlarına entegre edilir.

- **Örnek:** Birden fazla kuruluş arasındaki işbirlikçi bir AI projesinde, her katılımcının başkalarıyla paylaşamayacağı hassas veri kümeleri olabilir. Gizliliği koruyan makine öğrenimi, bu kuruluşların diğer taraflara hiçbir ham veriyi ifşa etmeden toplu verileri üzerinde paylaşılan bir AI modeli eğitmelerine olanak tanır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

5. Veri Maskeleme ve Belirteçleme

Veri maskeleme ve belirteçleme, hassas veri öğelerini maskelenmiş veya belirteçlenmiş değerlerle değiştirerek gizleyen tekniklerdir. Yapay zeka modelleri, bu gizlenmiş verileri işleyerek, orijinal hassas bilgilere doğrudan erişmeden değerli içgörüler çıkarabilir. Bu, hassas verilerin analiz için gerekli olduğu ancak yasal veya uyumluluk nedenleriyle ifşa edilemediği durumlarda özellikle yararlıdır.

- **Örnek:** Müşteri hizmetleri AI sisteminde, müşteri kredi kartı bilgileri analiz sırasında gizlenebilir. AI sistemi

6. Bağlamsal Bütünlük ve Politika Uygulaması

Yapay zeka, hassas bilgilerin yalnızca yetkili bağlamlarda kullanılmasını sağlayarak veri gizliliğini de artırabilir. Bağlamsal bütünlük, veri kullanımının önceden tanımlanmış politikalar ve gizlilik düzenlemeleriyle uyumlu olmasını sağlar. Yapay zeka sistemleri, verilerin bir kuruluş genelinde nasıl erişildiğini, kullanıldığını ve paylaşıldığını izleyerek gizlilik politikasının uygulanmasını otomatikleştirebilir.

- **Örnek:** Bir sağlık ortamındaki yapay zeka destekli bir sistem, hassas hasta verilerine yalnızca yetkili sağlık hizmeti sağlayıcıları tarafından ve yalnızca tedavi veya faturalama gibi belirli bağlamlarda erişilmesini sağlayabilir. Bir kullanıcı ilgisiz amaçlar için verilere erişmeye çalışırsa, yapay zeka sistemi HIPAA gibi gizlilik düzenlemelerine uyumu sağlamak için isteği işaretleyebilir veya engelleyebilir.

7. Otomatik Gizlilik Denetimi ve Uyumluluk

Yapay zeka, verilerin nasıl kullanıldığı ve paylaşıldığına ilişkin denetimi otomatikleştirerek kuruluşların gizlilik uyumluluğunu korumasına yardımcı olabilir. Yapay zeka modelleri, kişisel verilerin kötüye kullanılmadığından ve GDPR (Genel Veri Koruma Yönetmeliği) ve CCPA (Kaliforniya Tüketici Gizlilik Yasası) gibi gizlilik düzenlemelerine uyduğundan emin olmak için günlükleri, erişim kayıtlarını ve veri akışını analiz edebilir.

- **Örnek:** Çeşitli yargı bölgelerinde kişisel verileri işleyen çok uluslu bir şirkette, AI, kişisel verilerin GDPR'ye uygun olarak saklandığından, işlendiğinden ve paylaşıldığından emin olmak için veri uygulamalarını sürekli olarak denetleyebilir. Bu, gizlilik ihlalleri riskini azaltır ve küresel düzenlemelere uyumun sağlanmasına yardımcı olur.

8. AI Destekli Şifreleme Anahtarı Yönetimi

Şifreleme, veri gizliliğini korumak için temel bir yöntemdir, ancak şifreleme anahtarlarını güvenli bir şekilde yönetmek hayati önem taşır. Yapay zeka, şifreleme anahtar yönetimini gen otomasyonuyla iyileştirebilir

- **Örnek:** Bir AI sistemi, bir bulut depolama sağlayıcısı için şifreleme anahtarlarının yaşam döngüsünü yönetebilir, şifreleme anahtarlarının düzenli olarak döndürülmesini, güvenli bir şekilde saklanmasını ve yalnızca yetkili sistemler tarafından erişilebilir olmasını sağlayabilir. AI alışılmadık erişim kalıpları tespit ederse, şifrelenmiş verilere yetkisiz erişimi önlemek için anahtarları otomatik olarak iptal edebilir veya yeniden verebilir.

9. Gizlilik İhlalleri İçin Tehdit Tespiti

Yapay zeka, gerçek zamanlı olarak olası gizlilik ihlallerini belirleyerek veri gizliliğini iyileştirebilir. Yapay zeka destekli izleme sistemleri, verilere nasıl erişildiğini, paylaşıldığını veya işlendiğini analiz edebilir ve

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

yetkisiz erişim, veri sızdırma veya şüpheli kullanıcı davranışı gibi bir gizlilik ihlalini gösterebilecek etkinlikleri tespit edebilir.

- **Örnek:** Bulut tabanlı bir hizmette, AI müşteri verilerine nasıl erişildiğini izleyebilir ve alışılmadık etkinlikleri, örneğin bir kullanıcının alışılmadık derecede büyük bir veri kümesini indirmeye veya kısıtlanmış dosyalara erişmeye çalışmasını işaretleyebilir. Bu, yetkisiz veri ifşasını önlemeye ve gizlilik korumasını sağlamaya yardımcı olabilir.

10. Gizliliği Koruyan Yapay Zeka Geliştirme için Sentetik Veriler

Yapay zeka, hassas kişisel bilgileri kaldırırken veya gizlerken gerçek dünya verilerini taklit eden sentetik veriler üretebilir. Bu sentetik veriler, gerçek hassas verileri ifşa etmeden yapay zeka modellerini eğitmek için kullanılabilir. Sentetik veriler orijinal verilerin istatistiksel özelliklerini korurken, bireylerin yeniden tanımlanması riskini ortadan kaldırarak gizliliği sağlar.

- **Örnek:** Bir sağlık hizmeti AI sisteminde, gerçek hasta kayıtlarından sentetik hasta verileri üretilebilir. Bu sentetik veriler daha sonra herhangi bir gerçek hasta sağlık bilgisini ifşa etmeden AI modellerini eğitmek ve test etmek için kullanılabilir, böylece model geliştirmeye izin verirken gizlilik korunur.

Çözüm

Yapay zeka, farklı gizlilik, birleşik öğrenme ve homomorfik şifreleme gibi gizliliği koruyan teknikleri uygulayarak veri gizliliğini önemli ölçüde artırabilir. Yapay zekayı şifrelemeyle birleştirerek kuruluşlar, hassas bilgilerin korunmasını sağlarken verileri güvenli bir şekilde işleyebilir ve analiz edebilir. Yapay zeka ayrıca uyumluluk denetimi, şifreleme anahtarı yönetimi ve tehdit tespiti gibi gizlilik yönetimi görevlerini otomatikleştirerek onu bakım için hayati bir araç haline getirir.

Gizlilik düzenlemeleri sıkılaştırıldıkça ve güvenli veri işleme ihtiyacı arttıkça, yapay zekanın veri gizliliğini koruma ve geliştirmedeki rolü daha da kritik hale gelecek.

Homomorfik Şifrelemenin Sınırları Nelerdir ?

Homomorfik şifreleme, şifrelenmiş veriler üzerinde şifresini çözmeden hesaplamalar yapılmasına olanak tanıyan ve veri gizliliğini koruyan güçlü bir kriptografik tekniktir. Ancak, önemli potansiyeline rağmen, homomorfik şifrelemenin pratik, büyük ölçekli uygulamalarda uygulanmasını zorlaştıran birkaç sınırlaması vardır. Bu sınırlamalar şunları içerir:

1. Performans ve Verimlilik

Homomorfik şifrelemenin en önemli sınırlamalarından biri **hesaplama yüküdür** . Homomorfik şifreleme kullanarak şifrelenmiş veriler üzerinde hesaplamalar yapmak aşırı kaynak yoğun bir işlemdir ve şifrelenmemiş veriler üzerinde aynı işlemleri yapmaktan çok daha yavaş olabilir. Şifreleme, hesaplama

- **Örnek:** Şifrelenmiş verilerdeki temel bir aritmetik işlem (toplama veya çarpma gibi) düz metin verilerindekinden binlerce kat daha uzun sürebilir. Bu, yüksek verim gerektiren gerçek zamanlı uygulamalar veya sistemler için homomorfik şifrelemeyi kullanışsız hale getirir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

2. Karmaşık Operasyonlar İçin Sınırlı Destek

Homomorfik şifreleme şemaları genellikle destekleyebilecekleri işlemlerin türleri ve karmaşıklığı açısından sınırlıdır. Homomorfik şifreleme şemalarının farklı türleri vardır, örneğin:

- **Kısmen Homomorfik Şifreleme (PHE):** Yalnızca bir tür işlemi destekler (örneğin toplama veya çarpma).
- **Biraz Homomorfik Şifreleme (SHE):** Şifreli metnin "yenilenmesini" gerektirmeden önce sınırlı sayıda işlemi destekler.
- **Tam Homomorfik Şifreleme (FHE):** İsteğe bağlı hesaplamaları (örneğin toplama, çarpma, mantıksal işlemler) destekler ancak yüksek bir hesaplama maliyetine sahiptir.

Şifrelenmiş veriler üzerinde teorik olarak sınırsız işlem yapılmasına izin veren tam homomorfik şifreleme (FHE) bile oldukça kaynak yoğun bir yöntemdir ve gerçek dünyadaki birçok uygulama için henüz pratik değildir.

- **Örnek:** Bir kuruluşun şifrelenmiş veriler üzerinde karmaşık bir makine öğrenimi modeli çalıştırması gerekiyorsa, FHE gerekli hesaplamaları destekleyebilir, ancak modelin eğitim süresi önemli ölçüde artacaktır ve bu da onu büyük veri kümeleri veya gerçek zamanlı uygulamalar için verimsiz hale getirecektir.

3. Anahtar Yönetimi Karmaşıklığı

Homomorfik şifreleme hala anahtar oluşturma, depolama ve erişim kontrolü gibi geleneksel şifreleme anahtarı yönetim uygulamalarını gerektirir. Ancak, homomorfik şifreleme genellikle daha karmaşık şifreleme ve şifre çözme süreçlerini içerdiğinden, anahtar yönetimi daha da zorlayıcı hale gelir.

- **Örnek:** Doğru tarafların doğru şifre çözme anahtarlarına erişiminin sağlanması ve bu anahtarların güvenli bir şekilde döndürülmesi önemli bir operasyonel yük getirebilir. Anahtar yönetimindeki herhangi bir güvenlik açığı, tüm homomorfik şifreleme sisteminin güvenliğini tehlikeye atabilir.

4. Büyük Şifreli Metin Boyutları

Homomorfik şifreleme ile şifrelenen veriler, şifreli metinlerle sonuçlanır.

- **Örnek:** Küçük bir metin dosyasını homomorfik şifrelemeyle şifrelemek, orijinal dosyadan birkaç kat daha büyük bir şifreli metinle sonuçlanabilir. Büyük miktarda şifreli veriyi depolamak ve iletmek, özellikle sınırlı depolama veya ağ kapasitesine sahip uygulamalar için maliyetli ve verimsiz olabilir.

5. Sınırlı Ticari Kabul

Homomorfik şifreleme yıllardır akademik araştırma konusu olmasına rağmen, mevcut performans sınırlamaları ve teknik karmaşıklığı nedeniyle ticari uygulamalarda henüz yaygın bir şekilde benimsenmemiştir. Birçok kuruluş ve geliştirici, uzmanlaşmış bilgi, araç ve altyapıya ihtiyaç duyması nedeniyle homomorfik şifrelemeyi mevcut sistemlere entegre etmeyi zor bulmaktadır.

- **Örnek:** Homomorfik şifreleme sağlık ve finans gibi hassas sektörler için umut vadetse de, pratik, hazır çözümlerin eksikliği büyük ölçekli ticari projelerde kullanımını sınırlamıştır. Birçok şirket, daha zayıf gizlilik garantileri sağlasalar bile daha iyi performans sunan daha az karmaşık şifreleme şemalarını tercih ediyor.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

6. Standardizasyon Eksikliği

Şu anda homomorfik şifreleme için yaygın olarak kabul görmüş bir standart yoktur, bu da farklı sistemler ve uygulamalar arasındaki birlikte çalışabilirliği zorlaştırır. Her homomorfik şifreleme şemasının kendine özgü özellikleri olabilir ve tekniği farklı ortamlarda uygulamak için evrensel bir yaklaşım yoktur.

- **Örnek:** Tescilli bir homomorfik şifreleme şeması kullanan bir şirket, şifrelenmiş verileri farklı bir şema kullanan başka bir şirketle paylaşırken zorluklarla karşılaşabilir. Standardizasyon olmadan, sistemler arasındaki veri alışverişi ve işbirliği daha komplike hale gelir

7. Uygulama Geliştirmede Yüksek Karmaşıklık

Homomorfik şifreleme kullanan uygulamalar geliştirmek, özel kriptografik bilgi ve uzmanlık gerektirir. Geleneksel şifreleme yöntemlerini kullanmak kadar basit değildir, bu da gerçek dünya uygulamalarında homomorfik şifrelemeyi etkili bir şekilde uygulayabilen ve yönetebilen geliştiricilerin ve kuruluşların sayısını sınırlar.

- **Örnek:** Güvenli bulut bilişimi veya gizliliği koruyan veri analitiği için homomorfik şifreleme uygulamak, geliştirme ekipleri arasında yaygın olarak bulunmayabilecek derinlemesine kriptografi bilgisi gerektirir. Sonuç olarak, homomorfik şifrelemeli sistemler oluşturmanın öğrenme eğrisi dik olabilir.

8. Ölçeklenebilirlik Zorlukları

Homomorfik şifreleme önemli miktarda hesaplama yükü içerdiğinden, büyük veri kümeleri veya yüksek frekanslı işlemler için iyi ölçeklenmeyebilir. Büyük verilerle uğraşan veya hızlı işleme gerektiren kuruluşlar, ciddi performans ödünleri olmadan homomorfik şifrelemeyi kullanmayı zor bulabilir.

- **Örnek:** Günde milyonlarca işlem gerçekleştiren bir finans kuruluşunda, tüm işlemlere homomorfik şifreleme uygulanması sistemi önemli ölçüde yavaşlatır ve gerçek zamanlı dolandırıcılık tespiti veya finansal raporlama için pratik olmayan bir hale getirir.

9. Belirli Kullanım Durumları İçin Esnekliğin Eksikliği

Homomorfik şifreleme veri gizliliğini korumada oldukça etkili olsa da, her türlü gizlilik koruma uygulaması için en iyi çözüm olmayabilir. Bazı durumlarda, diferansiyel gizlilik, federasyonlu öğrenme veya güvenli çok taraflı bilgi işlem gibi diğer gizlilik artırıcı teknolojiler

- **Örnek:** Birden fazla merkezi olmayan veri kümesinden öğrenmesi gereken bir makine öğrenimi modeli, homomorfik şifrelemeden ziyade federasyonlu öğrenmeden daha fazla faydalanabilir, çünkü federasyonlu öğrenme, modelin merkezi işleme için verileri şifrelemeye ve şifresini çözmeye gerek kalmadan yerel olarak eğitilmesine olanak tanır.

Çözüm

Homomorfik şifreleme, gizliliği koruyan hesaplama ve güvenli veri işleme için umut verici çözümler sunar. Ancak, özellikle performans, hesaplama verimliliği, şifreli metin boyutu ve karmaşıklık açısından sınırlamaları, büyük ölçekli veya gerçek zamanlı uygulamalarda uygulanmasını zorlaştırır. Homomorfik şifrelemedeki

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

araştırmalar ilerledikçe, verimliliğinde ve daha geniş bir şekilde benimsenmesinde gelişmeler görebiliriz, ancak şimdilik önemli pratik engelleri olan niş bir teknoloji olmaya devam ediyor.

Federasyonlu öğrenme gizliliği nasıl artırır?

Federasyonlu öğrenme (FL), makine öğrenimi modellerinin, altta yatan ham verileri paylaşma veya merkezileştirme ihtiyacı olmadan birden fazla merkezi olmayan cihaz veya sunucuda eğitilmesini sağlayarak gizliliği artırır. Bunun yerine

1. Veri Yerelliği

Federasyonlu öğrenmede, veriler **kullanıcının cihazında** (veya yerel sunucuda) kalır ve asla merkezi bir sunucuya aktarılmaz. Her katılımcı cihaz, modeli kendi verileri üzerinde yerel olarak eğitir ve yalnızca güncellenen model parametreleri (eğimler) toplama için merkezi sunucuya geri gönderilir. Bu, kişisel bilgiler, sağlık kayıtları veya finansal işlemler gibi hassas verilerin cihazda kalmasını ve harici sistemlere açık olmamasını sağlar.

- **Örnek:** Tahmini metni geliştirmek için federasyonlu öğrenmeyi kullanan bir mobil uygulamada, kullanıcı yazma verileri her akıllı telefonda yerel olarak işlenir. Kullanıcıların metin verileri cihazlarından asla çıkmaz, böylece

2. Ham Veriler Yerine Model Güncellemeleri

Federasyonlu öğrenme sistemleri, ham verilerin kendisi yerine **model güncellemelerini** (ağırlıklar veya eğimler gibi) paylaşır. Bu güncellemeler yerel verilerden türetilir ancak orijinal veri noktalarını ortaya çıkarmaz, bu da herhangi birinin hassas bilgileri doğrudan güncellemelerden çıkarmasını zorlaştırır.

- **Örnek:** Hastanelerin hastalık tahmini için bir modeli işbirlikçi bir şekilde eğitmek için federasyonlu öğrenmeyi kullandığı bir sağlık sisteminde, her hastanenin hasta verileri gizli kalır. Yalnızca verilerdeki kalıpları yansıtan model güncellemeleri (bireysel kayıtları ifşa etmeden) paylaşılır ve küresel modeli iyileştirmek için toplanır.

3. Toplama ve Merkeziyetsizlik

Federasyonlu öğrenmede, merkezi sunucu yalnızca birden fazla katılımcıdan toplanan model güncellemelerini alır. Bireysel cihazlardan veya sunuculardan gelen güncellemeler, küresel modeli güncellemek için birleştirilir ve bu da herhangi bir güncellemeyi belirli bir bireye veya cihaza kadar izlemeyi daha da zorlaştırır. **Güncellemelerin bu şekilde toplanması,** yeniden tanımlama riskini azaltarak her kullanıcının verilerinin gizliliğini daha da korur.

- **Örnek:** 10.000 akıllı telefon yüz tanıma için federasyon öğrenme modeline güncellemeler katkıda bulunursa, merkezi sunucu tüm güncellemeleri toplar ve bu da belirli bir güncellemeyi tek bir kullanıcının verilerine kadar izlemeyi zorlaştırır, hatta güncellemelerden biri tehlikeye girse bile.

4. Farklı Gizlilik

Federasyonlu öğrenme, gizliliği daha da artırmak için farklı gizlilik teknikleriyle birleştirilebilir . Farklı gizlilik, model güncellemelerine paylaşılmadan önce rastgele gürültü ekleyerek güncellemelerin bireyler

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

hakkında hassas bilgileri çıkarmak için kullanılamamasını sağlar. Birisi güncellemelere erişim sağlasa bile, gizliliği korumak için eklenen gürültü nedeniyle herhangi bir kullanıcı hakkında anlamlı bilgi çıkaramaz.

- **Örnek:** Akıllı ev cihazları için bir uygulamada, her bir evin cihazından gönderilen güncellemelere farklı gizlilik uygulanabilir; böylece kötü niyetli bir aktör bu güncellemeleri engellese bile herhangi bir haneye ait verileri veya davranışları yeniden yapılandıramaz.

5. Güvenli Toplama

Merkezi sunucunun bireysel model güncellemelerini denetlemesini önlemek için, federasyonlu öğrenme güvenli toplama tekniklerini kullanabilir . Güvenli toplamada, bireysel cihazlardan gelen güncellemeler şifrelenir ve yalnızca toplanan sonuç (örneğin, tüm güncellemelerin toplamı) sunucu düzeyinde şifresi çözülür. Bu, merkezi sunucunun bile bireysel model güncellemelerini görememesini veya değiştirememesini sağlar.

- **Örnek:** Birden fazla bankanın bir dolandırıcılık tespit modeli eğitmek için federasyon öğrenimine katıldığı bir finansal hizmetler uygulamasında, güvenli toplama her bankanın güncellemelerinin şifrelenmesini sağlar. Merkezi sunucu yalnızca toplanan güncellemelere erişebilir, bu nedenle bireysel bankaların verileri özel kalır.

6. Azaltılmış Saldırı Yüzeyi

Federasyonlu öğrenme verileri merkezden uzak tuttuğu için veri ihlalleri riski azalır. Geleneksel makine öğrenmesi genellikle merkezi veri kümeleri gerektirir ve bu da onları saldırganlar için çekici hedefler haline getirir. Federasyonlu öğrenmede, veriler ayrı cihazlarda kaldığı için saldırı yüzeyi tek bir merkezi sunucuda yoğunlaşmak yerine birçok cihaza dağıtılır. Bu, saldırganların büyük miktarda hassas veriyi tehlikeye atmasını çok daha zor hale getirir.

- **Örnek:** Akıllı bir şehir sisteminde, çeşitli IoT cihazlarından (trafik sensörleri, kameralar ve enerji sayaçları gibi) gelen veriler, verileri merkezileştirmeden şehir yönetimini iyileştirmek için kullanılır. Bir cihaz tehlikeye girerse, yalnızca o belirli cihazdaki veriler risk altında olur ve bu da bir ihlalin genel etkisini en aza indirir.

7. Merkezi Kötüye Kullanıma Karşı Koruma

Federasyonlu öğrenme, merkezi otoriteler tarafından verilerin kötüye kullanılmasına veya suistimal edilmesine karşı koruma sağlar. Geleneksel sistemlerde, merkezi varlık tüm verilere erişebilir ve potansiyel olarak bunları kötüye kullanabilir (kasıtlı veya kasıtsız). Federasyonlu öğrenme ile, merkezi varlık yalnızca model güncellemeleri alır ve bu da katılımcılardan hassas bilgileri çıkarsama yeteneğini önemli ölçüde sınırlar.

- **Örnek:** Farklı üniversiteler arasında işbirlikli bir araştırma projesinde, federasyonlu öğrenme her kurumun kendi verileri üzerinde kontrol sahibi olmasını sağlar. Araştırma modelini yöneten merkezi sunucunun hiçbir ham öğrenci veya araştırma verisine erişimi yoktur, bu da yetkisiz kullanım riskini azaltır.

8. Veri Uyumluluğu Risklerinin Azaltılması

Federasyonlu öğrenme, kuruluşların GDPR (Genel Veri Koruma Yönetmeliği) ve **CCPA** (Kaliforniya Tüketici Gizlilik Yasası) gibi katı veri gizliliği düzenlemelerine uymasına yardımcı olur . Veriler yerel cihazda kaldığı ve paylaşılmadığı için, federasyonlu öğrenme, kuruluşların bu düzenlemelerin yasal sınırları içinde kalırken hassas veriler üzerinde AI modelleri eğitmesine olanak tanır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Avrupa merkezli bir tıbbi araştırma organizasyonu, birden fazla hastaneden hasta verilerini kullanarak hastalıkları teşhis etmek için AI modelleri geliştirmek amacıyla federasyonlu öğrenmeyi kullanabilir. Hasta verilerini yerinde tutarak ve yalnızca model güncellemelerini paylaşarak organizasyon, GDPR'nin veri ikametgahı ve gizlilik gerekliliklerine uyabilir.

Gizlilik Korumasında Federasyonlu Öğrenmenin Sınırlamaları

Federasyonlu öğrenme gizliliği artırırken, sınırlamaları da yok değil:

1. **Çıkarım Saldırıları:** Sadece model güncellemeleri paylaşılsa bile saldırganlar , özellikle katılımcı sayısı azsa, güncellemelerden hassas bilgileri yeniden oluşturmak için **çıkarım saldırıları** başlatabilir .
2. **Güvenli Toplama İşlemini Atlatma:** Güvenli toplama teknikleri uygulanmazsa veya toplama sürecinde güvenlik açıkları varsa, saldırganlar veya kötü niyetli merkezi sunucular yine de bireysel katkıları çıkarabilir.
3. **Cihazlardaki Kaynak Sınırlamaları:** Federasyonlu öğrenme, yerel cihazların hesaplama gücüne dayanır. Bazı cihazların sınırlı işleme yetenekleri olabilir ve bu da özellikle karmaşık modeller için federasyonlu öğrenmeye etkili bir şekilde katılmayı zorlaştırır.

Çözüm

Federasyonlu öğrenme, verileri merkezden uzak tutarak, ham veriler yerine yalnızca model güncellemelerini ileterek ve farklı gizlilik ve güvenli toplama gibi teknikleri kullanarak gizliliği önemli ölçüde artırır. Kuruluşların gizlilik düzenlemelerini ihlal etmeden veya hassas bilgileri ifşa etmeden makine öğrenimi projelerinde işbirliği yapmalarını sağlar.

Federatif öğrenmede model zehirlenmesinin riskleri nelerdir?

Federasyonlu öğrenmede model zehirlenmesi, kötü niyetli bir katılımcının eğitim süreci sırasında yanlış veya zararlı güncellemeler sunarak modeli kasıtlı olarak manipüle ettiği bir saldırı türünü ifade eder. Federasyonlu öğrenme, merkezi olmayan verilere ve birçok katılımcıdan gelen yerel güncellemelere dayandığından, uygun güvenlik önlemleri alınmazsa bu tür saldırılara karşı savunmasızdır. Model zehirlenmesi, önyargılı, yanlış veya hatta zararlı model davranışına yol açabilir.

Federasyonlu öğrenmede model zehirlenmesinin temel riskleri şunlardır:

1. Model Doğruluğunun Bozulması

Bir model zehirleme saldırısında, kötü niyetli katılımcılar modelin doğruluğunu düşürmek için yanlış veya yanıltıcı veriler sunabilirler. Hatalı güncellemeler besleyerek veya eğitim için kullanılan yerel verileri manipüle ederek, küresel modelin genel performansını düşürebilir, bu da yanlış sınıflandırmaya, yanlış tahminlere veya modelin çıktısına dayalı zayıf kararlara yol açabilir.

- **Örnek:** Hastanelerin hastalık tespiti için bir model eğitmek üzere işbirliği yaptığı bir federasyon öğrenme sisteminde, kötü niyetli bir katılımcı belirli bir hastalığı yanlış sınıflandıran zehirli güncellemeler sunabilir. Bu, modelin genel doğruluğunu azaltır ve klinik uygulamalarda güvenilmez hale getirir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

2. Arka Kapı Saldırıları

Model zehirlenmesinin daha tehlikeli biçimlerinden biri , kötü niyetli bir katılımcının modeli çoğu durumda normal şekilde çalışacak şekilde sinsice zehirlediği ancak belirli tetikleyici girdileri verildiğinde kötü niyetli davrandığı **arka kapı saldırısıdır . Genellikle saldırgan tarafından oluşturulan bu girdiler, modelin yanlış veya önyargılı kararlar almasına neden olur.**

- **Örnek:** Otonom araçlar için görüntü tanımayı iyileştirmek için kullanılan bir federasyon öğrenme sisteminde, bir saldırgan, belirli bir çıkartma tabelaya yerleştirildiğinde dur işaretlerini yanlış tanımlamasına neden olan bir arka kapı modele yerleştirebilir. Bu, kazalara veya diğer güvenlik tehlikelerine yol açabilir.

3. Önyargı Girişi

Kötü niyetli katılımcılar, belirli sonuçları orantısız şekilde etkileyen zehirli verileri besleyerek küresel modeli önyargılı hale getirebilir. Örneğin, bir saldırgan, modeli belirli sınıfları, demografik bilgileri veya davranışları kayırmak veya kayırmamak için yerel verileri manipüle edebilir.

- **Örnek:** Bankaların kredi dolandırıcılığını tespit etmek için kullandığı bir federasyon öğrenme sisteminde, kötü niyetli bir katılımcı, belirli demografik gruplardan gelen işlemleri diğerlerinden daha sık olarak sahte olarak işaretlemesine neden olan önyargılı veriler sunarak modeli zehirleyebilir ve bu da ayrımcılığa yol açabilir.

4. Tespitten Kaçınma

Federasyonlu öğrenme genellikle birçok katılımcıdan gelen güncellemeleri toplar ve bazı toplama yöntemleri (ortalama gibi) kötü amaçlı güncellemelerin kolayca tespit edilmeden genel modele karışmasına izin verebilir. Saldırganlar, özellikle çok sayıda katılımcı varsa ve saldırgan tarafından getirilen değişiklikler küçükse, anormallik tespit mekanizmalarından kaçan ince değişiklikler getirebilir.

- **Örnek:** Kötü niyetli bir katılımcı, anormal güncellemeleri işaretleyen algılama sistemlerini tetiklemekten kaçınmak için küçük değişiklikler yaparak, eğitimin birkaç yinelemesi boyunca modeli kademeli olarak zehirleyebilir. Bu yavaş zehirleme yaklaşımı, saldırganın hedeflerine zamanla ulaşmasını sağlarken saldırının fark edilmesini zorlaştırır.

5. Federasyonlu Öğrenme Sürecine Güven Kaybı

Federasyonlu bir öğrenme sistemindeki katılımcılar modelin zehirlendiğini keşfederse, bu tüm işbirlikli öğrenme sürecine olan güveni zedeleyebilir. Katılımcılar, verilerinin veya katkılarının kendi çıkarlarına aykırı olarak kullanıldığından korkabilir ve bu da gelecekteki federasyonlu öğrenme çabalarına katılma konusunda isteksizliğe yol açabilir.

- **Örnek:** Tedarik zinciri optimizasyonu için federasyonlu öğrenme modelini kullanan işletmeler, bir rakibin kendilerine olumsuz tavsiyelerde bulunmak için modeli zehirlediğini keşfederse, katılımcıların tüm ağı sürece olan güvenini kaybedebilir ve bu da nihayetinde federasyonlu öğrenme girişiminin başarısız olmasına yol açabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

6. Saldırgan Saldırılara Karşı Artan Güvenlik Açığı

Bir modeli zehirlemek, saldırganların kötü amaçlı amaçlar için modeldeki zayıflıkları istismar etmesini kolaylaştırarak, onun düşmanca saldırılara karşı sağlamlığını zayıflatabilir. Zehirlenen modeller, modelin zehirlenmemiş bölgelerinde bile, yanlış tahminlere veya çıktılara neden olan düşmanca girdilere karşı daha duyarlı hale gelebilir.

- **Örnek:** Federasyonlu bir öğrenme sisteminde

7. Hedefli Saldırılar

Bazı durumlarda saldırganlar genel modeli bozmak istemeyebilir, bunun yerine belirli kullanıcıları veya veri alt kümelerini hedeflemeye odaklanabilir. Saldırganlar, modeli yalnızca belirli girdi veya davranış türlerini etkileyecek şekilde sinsice zehirleyerek, tespit edilmesi zor ve belirli kullanıcılar için ciddi sonuçları olan hedefli saldırılar gerçekleştirebilir.

- **Örnek:** Sağlık hizmeti federasyonlu öğrenme sisteminde, bir saldırgan, belirli kanser tedavi türlerini yanlış sınıflandıracak şekilde modeli zehirleyebilir ve bu da, o kanser türüyle teşhis edilen hastalar için uygunsuz tedavi önerilerine yol açabilir.

8. Yanıltıcı Küresel Model Güncellemeleri

Federasyonlu öğrenmede, sunucu küresel modeli iyileştirmek için birden fazla istemciden gelen güncellemeleri toplar. Kötü niyetli istemciler, toplama sürecini yanıltan yanlış güncellemeler gönderebilir. Bu, modeli doğru öğrenmeden uzaklaştıran, hesaplama kaynaklarını boşa harcayan ve potansiyel olarak modelin en iyi olmayan veya yanlış çözümlere yakınsamasına neden olan güncellemelerle sonuçlanabilir.

- **Örnek:** Dil işleme için federasyonlu bir öğrenme kurulumunda, bir saldırgan, modeli belirli kelime tahminlerini veya çevirileri kayıracak şekilde çarpıtan güncellemeler gönderebilir ve böylece modelin doğru metin üretme becerisini genel olarak düşürebilir.

9. Gizlilik Riskleri

Model zehirlenmesi, özellikle zehirlenme saldırısı modelin katılımcıların yerel verileri hakkında hassas bilgileri ifşa etmesiyle sonuçlanırsa, gizlilik risklerine de yol açabilir. Bir saldırgan, modelin davranışını manipüle ederek, modeli ifşa etmemesi gereken bilgileri ifşa etmeye zorlayabilir ve bu da gizliliği tehlikeye atabilir.

- **Örnek:** Hastaneler tarafından kullanılan bir federasyon öğrenme sisteminde, kötü niyetli bir aktör, modeli kandırarak, yanlışlıkla özel verileri ifşa eden çıktılar üretmesini sağlayarak hastaların tıbbi durumları hakkında hassas bilgileri ortaya çıkarmak için bir zehirleme saldırısı tasarlayabilir.

Federasyonlu Öğrenmede Model Zehirlenmesine Karşı Savunmalar

Model zehirlenmesiyle ilişkili riskleri azaltmak için, federasyon öğrenme sistemleri çeşitli savunma mekanizmaları uygulayabilir:

1. **Sağlam Toplama Teknikleri:** Standart toplama yöntemleri (ortalama gibi) aykırı değerlere veya kötü amaçlı güncellemelere karşı savunmasızdır. **Medyan tabanlı toplama** , **Krum** veya **kırpılmış**

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

ortalama gibi sağlam toplama teknikleri , aşırı güncellemeleri göz ardı ederek veya sınırlayarak zehirli güncellemelerin etkisini en aza indirmeye yardımcı olur.

2. **Anomali Algılama: Sistemler, katılımcılardan gelen anormal güncellemeleri belirlemek ve filtrelemek için aykırı değer algılama** yöntemlerini kullanabilir . Kümeleme veya istatistiksel analiz gibi makine öğrenimi teknikleri, çoğunluktan önemli ölçüde sapan güncellemeleri belirlemeye yardımcı olabilir.
3. **İtibar Sistemleri:** İtibar tabanlı sistemler, katılımcılara zaman içindeki davranışlarına göre güven puanları atayabilir. Bir katılımcı sürekli olarak şüpheli güncellemeler gönderirse, güncellemelerine daha az ağırlık verilebilir veya toplama sürecinden hariç tutulabilir.
4. **Güvenli Çok Taraflı Hesaplama (SMPC): Güvenli çok taraflı hesaplama** gibi kriptografik teknikleri kullanarak , federasyon öğrenme sistemleri güncellemelerin güvenli bir şekilde işlenmesini sağlayabilir ve saldırganların tespit edilmeden güncellemeleri manipüle etmesini zorlaştırabilir.
5. **Farklı Gizlilik:** Öncelikle bireysel veri gizliliğini korumayı amaçlasa da **farklı gizlilik** , model zehirlenmesinin etkisini sınırlamaya da yardımcı olabilir. Güncellemelere rastgele gürültü ekleyerek, küçük ölçekli zehirlenme saldırılarının etkinliğini azaltabilir.
6. **Bizans Dayanıklı Algoritmalar:** Bu algoritmalar, federasyonlu bir öğrenme sisteminde kötü niyetli katılımcıları ele almak için tasarlanmıştır. Bizans dayanıklı algoritmalar, belirli sayıda kötü niyetli veya hatalı katılımcının varlığında bile küresel modelin sağlam kalmasını sağlamayı amaçlar.

Çözüm

Model zehirlenmesi, model doğruluğunu düşürebilen, önyargılar oluşturabilen veya hatta arka kapı saldırılarına olanak sağlayabilen federasyonlu öğrenmede önemli bir risktir. Federasyonlu öğrenme sürecine olan güveni zayıflatabilir ve modeli düşmanca saldırılara karşı savunmasız hale getirebilir. Ancak, sağlam toplama, anormallik tespiti ve Bizans'a dayanıklı algoritmalar gibi çeşitli savunma mekanizmaları, bu riskleri azaltmak ve federasyonlu öğrenmenin gizliliği koruyan makine öğrenimi için uygulanabilir bir yaklaşım olmaya devam etmesini sağlamak için kullanılabilir.

Federasyon öğrenmede yaygın saldırılar nelerdir?

Federasyonlu öğrenme (FL), gizliliği koruyarak artırır

1. Model Zehirleme Saldırıları

Model zehirlenme saldırısı

- **Model Zehirlenmesinin Türleri:**
  - **Arka Kapı Saldırıları:** Saldırgan, modeli çoğu durumda normal şekilde davranacak şekilde sinsice zehirler, ancak belirli girdiler veya tetikleyiciler sağlandığında kötü niyetli davranır (örn.
  - **Rastgele Zehirleme:** Saldırgan, model güncellemelerine rastgele gürültü sokar.
- **Örnek:** Spam tespiti için kullanılan bir federasyon öğrenme modelinde, kötü niyetli bir katılımcı modeli zehirleyerek belirli spam'lerin

2. Veri Zehirleme Saldırıları

Veri zehirleme saldırısında, kötü niyetli bir katılımcı yerel veri setini şu şekilde değiştirir:

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Örnek:** Sağlık hizmetleri için federasyonlu bir öğrenme sisteminde, bir saldırgan, modelin belirli tedavilerin sonucunu yanlış tahmin etmesini sağlamak için hasta verilerini değiştirebilir ve bu da hatalı tıbbi verilere yol açabilir.

3. Çıkarım Saldırıları

Çıkarım saldırıları, federasyonlu öğrenme sistemindeki diğer katılımcılar tarafından kullanılan veriler hakkında hassas bilgileri çıkarmayı amaçlar. Ham veriler

- **Çıkarım Saldırılarının Türleri:**
  - **Üyelik Çıkarım Saldırısı:** Saldırgan,
  - **Özellik Çıkarımı Saldırısı:** Saldırgan, katılımcıların yerel veri kümelerinin belirli özelliklerini veya karakteristiklerini çıkarsamaya çalışır.
- **Örnek:** Bir saldırgan, yüz tanıma için kullanılan bir federasyon öğrenme sistemindeki model güncellemelerini analiz ederek,

4. Bedavacı Saldırıları

Ücretsiz binici saldırısında, bir katılımcı eğitim sürecine herhangi bir yararlı güncelleme katkıda bulunmadan küresel modelden faydalanır. Saldırgan,

- **Örnek:** Otonom öğrenmeyi optimize etmek için federasyonlu bir öğrenme sisteminde

5. Kaçınma Saldırıları (Düşmanca Saldırılar)

Saldırgan saldırılar, kaçınma saldırıları olarak da bilinir ve dikkatlice hazırlanmış girdilerin f'ye gönderilmesini içerir.

- **Örnek:** Görüntü sınıflandırması için kullanılan bir federasyon öğrenme sisteminde, bir saldırgan insanlara normal nesneler gibi görünen ancak modelin yanlış etiketleme yapmasına neden olan saldırgan görüntüler oluşturabilir.

6. Bizans Saldırıları

Bizans

- **Örnek:** Sahtekarlık tespiti için federasyonlu bir öğrenme sisteminde, Bizans saldırganı, modelin sahtekarlık işlemlerini tespit etme yeteneğini azaltmaya çalışan güncellemeler gönderebilir ve bu da potansiyel olarak daha fazla sahtekarlığa izin verebilir.

7. Sybil Saldırıları

Bir Sybil saldırısında, saldırgan, sisteme katılmak için birden fazla sahte kimlik (Sybil düğümü) oluşturur.

- **Örnek:** Finansal risk tahmini için federasyonlu bir öğrenme sisteminde, bir saldırgan birkaç sahte onay işareti oluşturabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

8. Aracı Saldırıları

Bir aracı saldırıda (MITM), bir düşman müdahale eder.

- **Örnek:** Bir saldırgan, katılımcının cihazı ile federasyon öğrenme sunucusu arasındaki iletişimi keserek, model güncellemelerini değiştirerek genel modele güvenlik açıkları sokar.

9. Gradient Sızıntı Saldırıları

Gradyan sızıntı saldırıları, bir

- **Örnek:** Tıbbi görüntü analizi için federasyonlu bir öğrenme sisteminde, bir saldırgan,

Kötü Amaçlı Güncelleme Enjeksiyonu

Kötü amaçlı bir güncelleme enjeksiyon saldırısında, saldırgan sahte veya hatalı güncellemeler enjekte eder.

- **Örnek:** Spam tespiti için federasyonlu bir öğrenme sisteminde, bir saldırgan, sistemi bozan güncellemeler enjekte edebilir.

Federasyondaki Saldırılara Karşı Savunma

Bu riskleri azaltmak için, federasyonlu öğrenme sistemleri

1. **Güçlü Toplama Teknikleri: Medyan tabanlı toplama** veya **Krum** gibi teknikler , aykırı veya zehirli katkıların etkisini azaltarak kötü amaçlı güncellemelerin etkisini azaltmaya yardımcı olabilir.
2. **Güvenli Çok Taraflı Hesaplama (SMPC):** Güvenli çok taraflı hesaplama, hizmetin güvenli bir şekilde yürütülmesini sağlar.
3. **Farklı Gizlilik:** Farklı gizlilik teknikleri, model güncellemelerine gürültü ekleyerek, bireysel veri noktalarının
4. **Anomali Algılama:** Anomali algılama sistemleri, önemli ölçüde sapma gösteren anormal veya şüpheli güncellemeleri belirleyip filtreleyebilir.
5. **İtibara Dayalı Sistemler:** İtibar sistemleri, katılımcıların davranışlarını izler.
6. **İletişimlerin Şifrelenmesi:** Katılımcılar ile sunucu arasındaki iletişimin şifrelenmesi (örneğin TLS kullanılarak), aracı saldırıların önlenmesini ve güncellemelerin güvenli bir şekilde iletilmesini sağlayabilir.
7. **Rastgele İstemci Seçimi:** Her eğitim turu için katılımcıların rastgele bir alt kümesinin seçilmesi, bir saldırganın modeli etkileyecek kadar katılımcıyı kontrol etme olasılığını azaltır ve bu da riski azaltır.

Güvenli Çok Taraflı Hesaplama (SMPC)

Güvenli Çok Taraflı Hesaplama (Secure Multiparty Computation - SMPC), birden fazla tarafın girişlerini gizli tutarken bir işlevi ortaklaşa hesaplamasına olanak tanıyan bir kriptografik tekniktir. SMPC protokolünde amaç, katılımcı tarafların özel verilerini birbirlerine veya harici taraflara ifşa etmeden bir sonucun (örneğin bir toplam veya daha karmaşık bir hesaplama) hesaplanmasıdır.

SMPC'nin Temel Özellikleri

1. Gizlilik: Her tarafın verileri gizli kalır ve işlem sırasında veya sonrasında diğer taraflara ifşa edilmez.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

2. Doğruluk: Hesaplama sonucu doğru olur, taraflar girişlerini paylaşmasalar bile.
3. Güvenlik: Bazı taraflar kötü niyetli veya tehlikeye girmiş olsa bile, diğer tarafların girişlerini öğrenemezler veya hesaplamayı manipüle edemezler.

SMPC Nasıl Çalışır?

1. Girdi Paylaşımı: Her taraf özel verilerini gizli parçalara böler ve bu parçaları diğer taraflara dağıtır.
2. Paylar Üzerinde Hesaplama: Hesaplama, orijinal girdiler yeniden oluşturulmadan bu gizli paylar üzerinde gerçekleştirilir.
3. Sonucun Yeniden Yapılandırılması: İşlemin sonunda, taraflar hesaplanan paylarını birleştirerek birbirlerinin girdilerini öğrenmeden nihai sonucu elde ederler.

SMPC'de Kullanılan Temel Teknikler

1. Gizli Paylaşımı: Bir sır, hiçbir bireysel parça sırrı ifşa etmeyecek şekilde birden fazla parçaya bölünür. Yalnızca yeterli sayıda pay bir araya getirildiğinde orijinal sır yeniden oluşturulabilir.
2. Homomorfik Şifreleme: Bu teknik, veriler şifreli haldeyken hesaplamalar yapılmasına olanak tanır.
3. Oblivious Transfer: Bir tarafın diğerine veri gönderdiği, ancak gönderenin hangi veriyi gönderdiğini bilmediği bir protokoldür.

SMPC'nin Uygulamaları

1. Gizliliği Koruyan Makine Öğrenimi: Hassas verileri merkezileştirmeden makine öğrenimi modellerini eğitin.
2. Özel Kümeler Arası Kesişim: Kümeler arasındaki kesişim hesaplanırken, kesişim dışındaki veriler ifşa edilmez.
3. Güvenli Müzayedeler: Tekliflerin yalnızca sonuç belirlendiğinde açığa çıktığı güvenli müzayedeler yürütün.
4. Güvenli Oylama: SMPC, bireysel oyların gizli tutulduğu güvenli ve özel oylama sağlar.
5. Finansal Veri Analizi: Bankalar, ham verileri paylaşmadan hassas finansal veriler üzerinde ortak analizler gerçekleştirebilir.

SMPC'nin Zorlukları

1. Performans Yükü: SMPC, merkezi yöntemlere kıyasla hesaplama yükü getirir ve bu nedenle daha yavaştır.
2. Karmaşıklık: SMPC protokollerinin uygulanması önemli ölçüde kriptografik uzmanlık gerektirir.
3. Ölçeklenebilirlik: Katılımcı sayısı arttıkça SMPC'nin karmaşıklığı ve iletişim yükü artar, bu da büyük sistemlerde daha az ölçeklenebilir hale getirir.
4. Sınırlı İşlevsellik: SMPC ile bazı hesaplama türleri daha zorlu ve kaynak gerektirici olabilir.

Sonuç

Güvenli Çok Taraflı Hesaplama (SMPC), birden fazla tarafın katılımıyla gizliliği koruyan hesaplamalar yapmaya olanak tanır. Hassas verilerin gizli kalmasını sağlarken doğru ve güvenli hesaplamalar yapılmasına izin verir. Performans, karmaşıklık ve ölçeklenebilirlik açısından bazı zorluklarla karşılaşsa da, SMPC'nin gizliliği artıran teknolojilerde önemli bir rol oynaması beklenmektedir.

SMPC ve homomorfik sistemlerin farkları nelerdir?

Güvenli Çok Taraflı Hesaplama (SMPC) ve **Homomorfik Şifreleme** (HE) her ikisi de gizli

1. Temel Yaklaşım

- **SMPC (Secure Multiparty Computation):** SMPC, birden fazla tarafta bir işlev ortaklaşa hesaplayabilmesi için tasarlanmıştır, ancak her hesabının girilen verileri gizli kalır. SMPC'de, onun

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

geçmişinin verilerini diğerleriyle paylaşmaktan bir hesaplama veritabanı ve programlama sonunda sadece nihai sonuç çıkar. Bu süreç, gizli ödeme birleştirme, kriptografik protokoller ve programlama sonrasında ödemelerin birleştirilmesiyle yapılır.

- **Homomorfik Şifreleme (HE):** Homomorfik şifreleme, kayıtlı şifreli haldeyken bile üzerinde programlama yapılmasına olanak sağlar. Veriler hiçbir şekilde şifre çözülmeden işlemler gerçekleştirilebilir ve sonuç olarak şifresiz olarak gerçekleştirilebilir. Homomorfik şifreleme, tek bir tarafın şifrelenmiş yönlendirilmiş işlemleri gerçekleştirmesine olanak tanır ve genellikle merkezi bir içerir.

2. Hakların Sayısı

- **SMPC:** SMPC genellikle birden fazla (iki veya daha fazla) süre arasında kalır. Her şeyin kendi gizli verisini paylaşmadan işlenmesinden ortaya çıkar. Program, programın dağıtıldığı şekilde ortak programlama boyunca devam eder.
- **Homomorfik Şifreleme:** Homomorfik şifreleme, tek bir taraf veya merkezi bir sistem şifreli verilerin üzerinde programlama yapılmasını sağlar. Bu durumda, şifrelenmiş veriyi tutan taraf veya işlem yapan taraf sayısı birden fazla olabilir, ancak verilerin tamamı şifrelenmiş haldedir ve sadece bir kişi veya sistem şifrelenmiş verilerle işlem yapar.

3. Gizlilik ve Veri Paylaşımı

- **SMPC:** SMPC'de, kişilerin birbirlerine veri göndermez. Her birinin gizli tutulmasını sağlamak için kriptografik protokolleri kullanılır. Veriler hiçbir zaman paylaşılmaz ve sadece işleyişin sonuçlarını açığa çıkaracak bilgi hesaplamalarını yapar.
- **Homomorfik Şifreleme:** Homomorfik şifrelemede, veriler şifrelenmiş halde kalır ve işlemi yapan tarafta asla verinin açık gösterimiz. Şifre çözülmemiş veriler üzerinde işlem yapılır. Şifrelen

4. Kullanım Senaryoları

- **SMPC:** SMPC, birden fazla tarafta işbirliği yaparak hesaplamalar gerçekleştirmesi gereken durumlar için uygundur. Örneğin, farklı şifrelerin güvenli bir şekilde gerçekleştiği (bankalar, sağlık sistemleri, vb.) verilerinin paylaşılmasından bir ortak model veya sonucun değişmesi gerekir.
- **Homomorfik Şifreleme:** Homomorfik şifreleme, genellikle bir tarafın verileri şifrelenmiş halde başka bir veri çıkışı ve bu tarafın veriyi deşifre edilmemesi işlemlerinin seyrinde kullanılır. Örneğin bir bulut servis sağlayıcısının ve

5. Performans

- **SMPC:** SMPC genellikle planlama açısından daha hızlıdır çünkü gizli paylaşım ve protokoller verileri arasında doğrudan bir işlem yapma olanağı tanır. Ancak, sayıları sayıları iletişim maliyetleri artabilir, çünkü her bölümün paylaşımında bulunmak mevcuttur.
- **Homomorfik Şifreleme:** Homomorfik şifreleme, programlama bakış açısı daha yavaş olabilir çünkü şifrelenmiş veriler üzerindeki çalıştırma işlemleri oldukça karmaşık ve ağırdır. Bu nedenle, çevresel homomorfik şifreleme genellikle daha zorludur ve büyük veri setlerinde performans sağlamak zor olabilir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

6. Güvenlik Garantileri

- **SMPC:** SMPC, kadınlarda kötü olabilecek durumlara karşı koruma sağlayabilir. Protokoller, herhangi bir fazla varlığın kapsadığı sistemlerde güvenliği sağlar ve belirli sayıdaki varlıkların kötü niyetli olmasına rağmen doğru sonuç elde edilebilir.
- **Homomorfik Şifreleme:** Homomorfik şifreleme, kayıtlı olarak şifrelenmiş halde tutulmasını sağlar ve yalnızca şifre çözücü anahtara sahip olan kişinin saklanabilir durumda görünmesini sağlar. Homomorfik şifreleme, şifre ayırmadan güvenli hesapl

7. Sonuçların Yayımlanması

- **SMPC:** SMPC'de her şeyin yalnızca ortak programlamanın sonucunu öğrenir; içeriğin hiçbir zaman ayrıntılarının özel sistemlerine erişilemezler.
- **Homomorfik Şifreleme:** Homomorfik şifrelemede, şifre çözme cihazını olan kişinin programlama sürecini deşifre ederek öğrenir. Ancak işlem yapan tarafın verilerinin ayrıntıları hiçbir zaman öğrenilemez.

Özet:

Özellik	SMPC	Homomorfik Şifreleme
Temel Yapı	Çok yönlü işbirlikçi programlama	Şifrelenmiş veriler üzerinde tek şifre programlama
yaratıcı olmak	İki veya daha fazla	Model bir taraf (veya merkezi sistem)
Gizlilik	Girdi verileri paylaşılmaz	Şifre çözülmeden işlemler yapılır
Performans	Daha hızlı, ancak iletişim maliyeti yüksek olabilir	Daha yavaş, şifrelenmiş veriler üzerinde işlem zorluğu
Güvenlik	Birden fazla tarafın kötü niyetli olmasına karşı dayanıklı	Veriler şifre çözülmeden güvenlidir
Sonuçların Yayımlanması	Sonuç tüm rotalarda ortaklaşa öğrenilir	Sonuç yalnızca şifreyi çözen taraftan öğrenilir

Her iki teknoloji de veri gizliliğini koruma ve güvenli programlama yapma konusunda güçlü çözümler sunmaktadır. Ancak kullanımları belirli senaryolara göre değişir; SMPC, birden fazla tarafın işbirliği yaptığı daha uygun, homomorfik kırılma ise bir tarafın verileri şifrelenmiş olarak işlemek zorunda olduğu durumlar için daha uygun bir yaklaşımdır.

Güvenli Çok Taraflı Hesaplama (SMPC) ve Homomorfik Şifreleme: Detaylı Karşılaştırma

Güvenli çok veri programlama (SMPC) ve homomorfik şifreleme (HE), iki farklı gizlilik sağlayan kriptografik teknik olup, her ikisinin de gizli gizli kalmasını sağlarken programlama yapılmasını sağlar. Bu iki yöntem arasındaki temel farkları, kullanım şekilleri ve birbirlerine göre avantajlarını, zorluklarını ve sınırlamalarını aşağıda 25-30 madde ile detaylandırarak açıklayalım.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

1. Temel Amaç ve Felsefe

- **SMPC** : Çoklu veri işbirliği yaparak gizli bölünmeyi paylaşmadan ortak bir programlama gerçekleştirmesini sağlar.
- **Homomorfik Şifreleme** : Bir tarafta şifrelenmiş kimlik erişim sağlamaktan, şifreyi ayırmaden programlamaların yapılmasına olanak sağlar.

2. İşleyiş Modeli

- **SMPC** : Hesaplamalar, birden fazla taraf işbirliğiyle yapılır. Katılımcıların eşitsizliğinden bir işlev hesapları.
- **Homomorfik Şifreleme** : Hesaplama, tamamen şifrelenmiş veri üzerinde yapılır. Şifrelenmiş doğrulama işlemleri devam ederken, sonuçlar şifresi çözülerek alınır.

3. Hakların Sınırı

- **SMPC** : iki veya daha fazla ka
- **Homomorfik Şifreleme** : Tek bir taraf veya merkezi bir sistem şifrelenmiş veri üzerinde programlamalar yapıldığında kullanılır.

4. Gizlilik Politikası

- **SMPC** : Verilerin gizliliği, programlama sırasında mevcut olan hiçbir veri paylaşılmaması sağlanır. Veriler ödeme gizlilaştırma ve protokollerle korunur.
- **Homomorfik Şifreleme** : Verilerin gizliliğinin şifrelenmesi işlemleri ile sağlanır. Veriler şifreli kalır ve kimse şifreyi değiştirmeden işlem yapamaz.

5. Kullanım Alanı

- **SMPC** : Gösterilen sağlık, finans, oylama gibi alanlarda fazla sayıda alanda ortak planlama yapılması gereken senaryolarda kullanılır.
- **Homomorfik Şifreleme** : Bulut tabanlı veri işleme, güvenli veri analizleri ve veri paylaşmadan merkezi sistemlerin analiz edilmesi gereken durumlar için uygundur.

6. Performans

- **SMPC** : Ürünlerin daha hızlıdır ancak kesintilere göre iletişim maliyeti artabilir.
- **Homomorfik Şifreleme** : Hesaplama ağırdır ve büyük veri setlerinde daha yavaş çalışır. Hesaplamalar daha fazla

7. Veri Paylaşımı

- **SMPC** : Hiçbir veri paylaşılmaz, yalnızca gizli ödemeler programlamaya dahil edilir.
- **Homomorfik Şifreleme** : Veriler şifrelenmiş halde kalır, şifre kesilmeden veri kimseyle paylaşılmaz.

8. Sonuç Yayımlanması

- **SMPC** : Sonuç olarak, tüm olanlar arasında paylaşılır. Ancak bireysel veriler gizli kalır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

- **Homomorfik Şifreleme** : Sadece şifreyi şifreleyenne sahip olan kişi sonuçları belirlenir.

9. Güvenlik Garantisi

- **SMPC** : Birden fazla uzatma olsa bile güvenlik protokolleriyle korunur. Kötü niyetli ayrıntıları programlamayı değiştiremez.
- **Homomorfik Şifreleme** : Veriler şifreli değildir, kimse bu yetkiye erişim sağlayamaz.

10. Gizli Ödeme

- **SMPC** : Her şeyin verisini gizli olarak böler ve diğer mevcutlarla paylaşır, ancak bu parçaların verinin ayrılamaması durumunda olmaz.
- **Homomorfik Şifreleme** : Verilerin tamamı şifrelenir, programlamalar şifre kesilmeden yapılır.

11. Esneklik

- **SMPC** : Birden fazla tarafın eklenmesiyle programların yapılması işbirliği açısından önemlidir, bu da esneklik sağlar.
- **Homomorfik Şifreleme** : Veril

12. Veri Bütünlüğü

- **SMPC** : Her tarafın verileri doğru şekilde işlenir, sonuç doğru şekilde elde edilir.
- **Homomorfik Şifreleme** : Hesaplamalar doğrudan şifrelenmiş veri üzerinde yapılır, sonuç doğrulukla korunur.

13. Saldırılara Karşı Dayanıklılık

- **SMPC** : Katılımcıların kötü niyetli olsa bile verimliliği, güvenliği sağlar.
- **Homomorfik Şifreleme** : Dışarıdan saldırılara karşı dayanıklı, verilerin şifrelenmiş şekilde erişime ulaşması sağlanamaz.

14. Adli Bilişim ve Veri Analizi

- **SMPC** : Birden fazla üyenin değiştirilmesi gerektiği için hukuk, adli bilişim ve veri analizi gibi alanlarda kullanılır.
- **Homomorfik Şifreleme** : Gizlilik, bulut tabanlı veri analizleri için uygundur.

15. Veri Büyüklüğü

- **SMPC** : Daha küçük veri setlerinde daha etkili olabilir.
- **Homomorfik Şifreleme** : Büyük veri setlerindeki zorluk

16. Zorluklar

- **SMPC** : Katılımcılar arasındaki iletişim ve güvenlik protokolleri karmaşıktır.
- **Homomorfik Şifreleme** : Şifrelenmiş veriler üzerinde işlem yapılmasıyla elde edilen yüksek işlem maliyeti vardır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

17. Ölçeklenebilirlik

- **SMPC** : Katılımcıda bozulmaya göre ölçeklenebilirlik düşebilir.
- **Homomorfik Şifreleme** : Tek şifre kodlamalar daha iyi ölçeklenebilir, ancak performans düşebilir.

18. Hassas Veri Yönetimi

- **SMPC** : Hassas verilerin birden fazla taraf arasında gizli tutulması gereken miktarlarda kullanılır.
- **Homomorfik Şifreleme** : Merkezi bir sistem hassas veriler üzerinde işlem yapılmasını sağlar.

19. Merkezi vs. Dağıtık Yaklaşım

- **SMPC** : Dağıtık ve işbirlikçi bir modeldir.
- **Homomorfik Şifreleme** : Merkezi bir işleme modeline dayanıklıdır.

20. Karmaşıklık

- **SMPC** : İletişim ve gizli paylaşım karmaşıktır.
- **Homomorfik Şifreleme** : Şifrelenmiş doğrulanmış işlemler zordur.

21. Kriptografik Derinlik

- **SMPC** : Daha geniş bir kriptografik yapıyı gerektirir, gizli paylaşım ve parçalara bölünebilir.
- **Homomorfik Şifreleme** : Daha ayrıntılı işlemler içerir, özellikle homomorfik programlama için optimize edilmesi gerekir.

22. Veri Gizliliği

- **SMPC** : Tüm kişisel verileri korur.
- **Homomorfik Şifreleme** : Veriler şifrelenmiş halde dışarıdan erişim mümkün değildir.

23. Sonuçların Hassasiyeti

- **SMPC** : Sonuçların tüm yönleri öğrenilebilir.
- **Homomorfik Şifreleme** : Sonuçlar sadece şifre çözmenize sahip olan kişi tarafından öğrenilir.

24. Güvenlik Protokolleri

- **SMPC** : Daha karmaşık güvenlik protokolleri içerir.
- **Homomorfik Şifreleme** : Daha az kompleks ancak daha yavaş şifreleme protokolleri içerir.

25. Yapay Zeka ve Makine Öğrenimi ile Entegrasyon

- **SMPC** : Çalışan makine geliştirme modellerinde birden fazla kurulum veriyle işbirliği içinde kullanılır.
- **Homomorfik Şifreleme** : Tek bir taraflı bulut veya merkez üzerinde veri işlemesi gereken makine yazılımları sistemlerinde kullanılır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

26. Hukuki Yapımlar

- **SMPC** : Verilerin birden fazla taraf arasında paylaşılması nedeniyle, çeşitli veri koruma seçenekleri ve biçimleriyle (örnek GDPR) uyumludur. Verilerin paylaşıldığı her şeyin maliyetini sağlar.
- **Homomorfik Şifreleme** : Verilerin şifrelenmiş olması, merkezi sistemlerin kullanımı sırasında veri güvenliği sağlanır ve bu da veri koruma düzenlemelerine

27. Veri Sahipliği

- **SMPC** : Her şeyin kendi verisinin sahibi olmaya devam eder, veriler başka bir yere gönderilmeden işlenir.
- **Homomorfik Şifreleme** : Veriler şifrelenmiş olarak işleme konur, fakat işleme sırasında kayıtlı olanın hangisi olduğu bilinmiyor ve sadece sonuç öğrenilir.

28.Şeffaflık

- **SMPC** : Tüm işlemlerin her adımında yer alır, programlamalar şeffaf ve denetlenebilir hale gelir.
- **Homomorfik Şifreleme** : Şifrelenmiş veriler üzerinde işlem yapılması için şeffaflık daha az ve en çok işlemler merkezi sistem tarafından açık tutulur.

29. Hatalara Dayanıklılık

- **SMPC** : Hesaplamalar aniden fazla tarafın sunumunu izlemek için, bir hesapların hata yapması durumunda programlama yanlış olabilir. Ancak protokoller kötü niyetli veya hatalı hataların oluşmasını sağlamak için optimize edilebilir.
- **Homomorfik Şifreleme** : Hesaplamalar tamamen şifreli veri üzerinde yapılır, bu nedenle hata yapma olasılığı daha düşüktür. Ancak şifrelenmiş veriyle işlem yapmak programlamayı daha karmaşık hale getirebilir.

30. Son Kullanıcı Güvenliği

- **SMPC** : Kullanıcılar arasında işbirliği sağlandığı için güvenlik seviyesi yüksek olup, birbirlerine güvenmese bile sonuç güvenli bir şekilde alınır.
- **Homomorfik Şifreleme** : Veri şifreliliği, tek bir taraflı programlamayı güvenli bir şekilde yürütülmesi garanti edilir.

Geniş Sonuç ve Değerlendirme

Güvenli Çok Taraflı Hesaplama (SMPC) ve Homomorfik Şifreleme (HE), her ikisini de gizliliği koruma amacı güden iki güçlü kriptografik tekniktir. Bu teknolojilerin bir araya gelmesi, çeşitli sektörlerde veri gizliliği ve güvenlik alanında yeni kapılar açmaktadır. Ancak bu iki teknolojik kullanım, belirli koşullar ve kullanım senaryolarına göre değişiklik gösterir. Mevcut SMPC ve Homomorfik Şifreleme'nin geniş sonuçları ve değerlendirmeleri sunulmaktadır:

1. Gizlilik Odaklı Yaklaşımlar

- Her iki teknolojinin de korunmasının korunması büyük önem verir.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

2. Performans ve Verimlilik

- Homomorfik şifrelemenin en büyük miktarı, program takvimi ve performans düşüklüğüdür. Büyük veri ayarlarında yavaş olabilir ve işlemler uzun zaman alabilir. Öte yandan, SMPC planlama stratejisi daha verimli olabilir, ancak bunlar arasındaki iletişim maliyetleri artabilir.

3. Kullanım Alanları

- SMPC, özellikle dağıtık sistemlerde, farklı paraların gizli paraların paylaşımından ortak bir analiz rejiminde kullanışlıdır. Homomorfik şifreleme ise bulut bilişim, güvenli veri analizi ve verinin korunmasının sağlanması durumları için uygundur.

4. Veri Koruma ve Düzenlemeler

- SMPC, özellikle veri korumasına uyumlu çalışmak isteyen kuruluşlar için uygun bir çözümdür. Örneğin,

5. Çok Taraflı İşbirliği

- SMPC, anlık olarak fazla miktarda sunumunu sağlar. Örneğin, sağlık sektöründe birden fazla hastanede kalmayı paylaşmadan bir AI modelini eğitmek için SMPC kullanabilir. Homomorfik şifreleme ise tek işlemler işlemleri için daha uygun ve kayıtlı merkezi bir sistem şifreli olarak çalıştırılmasını sağlar.

6. Veri Gizliliği

- Her iki teknolojide de gizlilik ve yüksek düzeyde korunur. Ancak SMPC, isteğe bağlı olarak fazla taraf arasında paylaşılmasından gereken senaryolarda tercih edilirken, homomorfik şifreleme, bir tarafın şifreli veriyi analiz etmesiyle daha uygundur.

7. Adli Bilişim Uygulamaları

- SMPC, birden fazla tarafın bloke edilmesinden işbirliği yapılması gereken adli bilişim ve yasal sürümlerde güçlü bir araç olabilir. Öte yandan, homomorfik depolama, hassas verilerin şifrelenmiş olarak incelenmesi gereken durumlar için idealdir.

8. Karmaşıklık ve Yatırım Maliyeti

- SMPC, kriptografik karmaşıklık açısından yüksek düzeyde bilgi gerektirirse de daha hızlı alınabilmesini sağlar. Homomorfik kırılma ise büyük miktarda işlem gücü ve zaman gerektirir, bu da yüksek büyümeyle sonuçlanabilir. Büyük verilerle çalışırken daha fazla kaynak uygulanabilir.

9. Yapay Zeka ve Makine Öğrenimi Entegrasyonu

- SMPC, yapay zeka ve makine düzenleyicileri sistemlerinde dağıtık veri kümeleriyle çalışmak için uygundur. Birden fazla programın bir araya getirilmesinden oluşan ortak modelin eğitilmesi gereken senaryolar için güçlü bir çözümdür. Homomorfik şifreleme ise, bulut tabanlı yapay zeka uygulamaları için verilerin şifrelenmiş olarak çalıştırılmasını sağlar.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231

10. Güvenlik

- Her iki teknoloji de saldırılara karşı dayanıklı olmakla birlikte, uygulama hataları ve performans sorunlarını güvenlik risklerini artırabilir. SMPC'de mevcut olanlar arasındaki iletişim ömrü kritik bir sürekliliktir. Homomorfik şifrelemede ise programlamaların karmaşıklığı güvenlik açıklarını, ancak performans maliyeti önemli bir faktördür.

Sonuç olarak, Güvenli Çok Taraflı Hesaplama (SMPC) ve Homomorfik Şifreleme (HE) veri gizliliği ve güvenlik sağlama açısından önemli araçlardır. SMPC, birden fazla taraf işbirliği içinde güvenli programlama yapmayı gerektiren senaryolarda ideal bir çözüm sunarken, homomorfik kırma, özellikle bulut bilişim ve merkezi veri işleme ortamlarında güçlü bir güvenlik sağlar. Her iki teknolojide veri gizliliği ve tasarrufu konusunda büyük bir potansiyel taşıyor ve gelecekte veri işleme ve güvenlik stratejilerinde önemli roller oynamaya devam edecek.

Bitirme Yazısı

Güvenli Çok Taraflı Hesaplama (SMPC) ve Homomorfik Şifreleme (HE), veri gizliliği ve güvenliğine yönelik artan ihtiyaçlara cevap veren iki ileri düzey kriptografik tekniktir. Her iki yöntemin gizli olarak saklanmasını sağlarken, veri üzerinde programlama yapma imkanı tanır. Ancak bu iki teknoloji farklı yaklaştı

SMPC, birden fazla tarafın piyasaya sürülmesiyle saklanmasını ve kişisel gizliliğini koruyarak dağıtık bir programlama yöntemi olarak öne çıkar. Tarafın kendi verisini gizli tutarak, işbirliği ile doğru şekilde çalışmasını sağlar. SMPC, özellikle sağlık, finans ve hukuk gibi hassas verilerin bulunduğu ve tüm sektörlerde etkin bir çözüm sunmaktadır.

Homomorfik Şifreleme ise kayıtlı şifreli haldeyken bile çalıştırılabilmesine olanak sağlar. Bu teknoloji, özellikle bulut tabanlı uygulamalarda büyük bir avantaj sağlayarak, veri merkezi bir platformda şifre ayırma işleminin yapılmasından gerçekleştirilmesine imkan verir. Ancak HE'nin yüksek işlem maliyeti ve performansın düşüklüğü gibi sınırlamaları, büyük veri setlerinde kapasitelerini zorlaştırabilir.

Bu iki teknoloji, her birinin kendi ve patlaması ile farklı güvenlik ihtiyaçları karşılar. SMPC, çok parçalı işbirliği şemalarında daha uygun bir çözüm sunarken, Homomorfik Şifreleme merkezi veri işlemede veri depolamalarını koruma konusunda güçlüdür. Her iki teknoloji de gelecekte veri güvenliği ve güvenliğinin vazgeçilmez parçaları olacak ve veri güvenliği konusunda sorun gidermeye uyum sağlamada öne çıkan

Sonuç olarak, SMPC ve Homomorfik Şifreleme, veri güvenliğinin sağlanması ve kişisel bilgilerin korunması için güçlü araçlardır. Her iki yöntemin, gizlilik ve güvenlik açısından sürekli olarak bozulma yapısı, ilerleyen yıllarda performansın daha yaygınlaşmasına izin verilmesi ve size kolaylık sağlaması. Bu nedenle, bu teknolojinin üzerinde yapılan çalışmalar ve düzenler, dijital dünyanın daha güvenli hale gelmesinde kilit bir rol oynayacaktır.

Selçuk DİKİCİ- Emdüstri Mühendisi
ORCID ID: 0009-0009-2691-3231