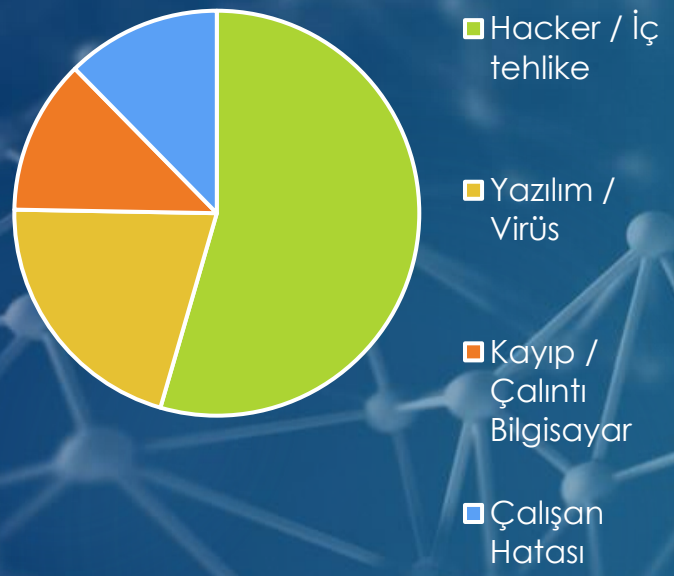
Siber Risk Oluşturan Başlıca Etkenler ve Sebepler

Risklerin Dağılımı



- ✓ Hacker/Bilgisayar Korsanları
- ✓ Kazara Sızma
- ✓ İçerdeki kötü niyetli kişiler (çalışanlar)
- ✓ Bütünü etkileyebilecek nitelikteki insan ve sistem kaynaklı hatalar

- ✓ Şifrelenmemiş taşınabilir cihazların kaybı
- ✓ Sahte e-postalar, fakslar, belgeler
- ✓ Dataların uygunsuz imha edilmesi
- ✓ Dijitalleşme
- ✓ Artan ara bağlantılar

- ✓ Teknik güvenlik arızaları, kötü tasarlanmış ve/veya muhafaza edilen bilgi güvenliği yönetim sistemleri (ISMS)
- ✓ Nesnelerin interneti (IoT-Internet of Things)
- ✓ Globalleşme

Bilgi Güvenliği Standartları

- **ISO / IEC 27000 ailesi arasında yer alan standartlar (örn. ISO 27001), bir Bilgi Güvenliği Yönetim Sistemi (Information Management Security Management System -ISMS) kurarak politika ve prosedürlerin yönetimi için ortak bir çerçeve tanımlamaktadır.**

- **NIST Siber Güvenlik Çerçevesi (NIST Cyber Security Framework)**

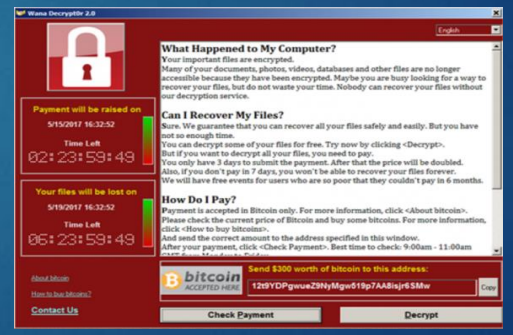
- **PCI DSS Seviyeleri**
  - Yılda 6 milyon Visa işlemi gerçekleştiren -kabul kanalı ne olursa olsun -herhangi bir tacir.
    Visa, kendi takdirine bağlı olarak, 1. Seviye tüccar gereksinimlerini karşılaması gereken herhangi bir tacir sisteminin riskini en aza indirgemek için tanımlamaktadır.
  - Yılda 1m ila 6 milyon arası -kabul kanalı ne olursa olsun -herhangi bir tacir.
  - Yılda 20.000 ila 1 milyon arası -kabul kanalı ne olursa olsun -herhangi bir tacir.
  - Yılda 20.000'den az Visa e-ticaret işlemi yapan herhangi bir tacir ve kabul kanalından bağımsız diğer tüm satıcılar – yılda 1 milyon'a kadar Visa işlemi gerçekleştiren.

Siber Saldırı Türleri

- DOS veya DDOS
- Kötü amaçlı yazılım
- Virüs saldırıları
- Yazılım Korsanlığı

- Pharming
- Yanıltıcı E-Posta
- Satın Alma Dolandırıcılıkları
- Çalıntı Bilgisayar
- USB Sürücüleri

- Endüstriyel Casusluk
- Siber Gasp
- Oltalama / Phishing
- Kişiye özel Oltalama



Siber Saldırının Başlıca Sonuçları

- Kritik verilerin kaybolması ve/veya bilgisayar sisteminin tehlikeye atılması.
- E-ticaretin kapatılması sonucunda müşteri kaybı.
- Medyada yer alan olumsuz haberler / İtibara gelen zarar
- Kara olumsuz etkisi / Hisse değerinin düşmesi / Şirketin azalan piyasa değeri
- Hırsızlık ve gasp
- Sözleşmelerin ihlali
- Ürün geri çağırma
- Düzenleyici kuruluşların yürüttüğü artan detaylı incelemeler ve bu incelemeler sonucu kesilen ciddi mali cezalar.
- Maddi zarar
- Kamu otoritelerinin başlatacağı işlemler ve ilişkili para cezaları
- Ticari sırların / gizli bilgilerin kaybı
- Bildirim Masrafları ve ilgili diğer masraflar
- Ağ Güvenliği Sorumluluğu

Teminat Kapsamında Olanlar

Teminat Sağlanan Konular

- Birinci Taraf Zararı
  - İş Durması
  - Bekleme Süresinin Aşılması
  - İyileştirme
  - Bilgisayar Korsanı Hırsızlığı
  - Siber Gasp Tehditleri
  - Acil durum masrafları
  - Kriz Yönetimi
  - Yasal veya Düzenlemeler Gereği İş Durması
- Üçüncü Şahıs Zararı
  - Mahremiyet İhlali
  - Gizlilik İhlali
  - Medya Hatalı Eylemi
  - Güvenlik Hatalı Eylemi
  - Düzenleyici Otorite Ceza ve Masrafları
  - İç Soruşturma Masrafları
  - Ödeme Kartı Endüstrisi Veri Güvenliği Standartları Teminatı

2019 yılından Siber Saldırı Örnekleri - 1

- Amerikan otel zinciri pasaport numaraları ve kredi kartı bilgileri dahil 383 milyon müşteri verisine saldırı yaşadı.
- Bir güvenlik araştırmacısı şirket hassas bilgi dolu sunucuların ne vaziyette olduğunu göstermek için bulut tabanlı bir sunucuda tam 773 milyon e-posta adresine erişim sağladı.
- Sosyal medya platformları ve çöpçatanlık sayfalarının da yer aldığı 16 web sayfasından 617 milyon kişiye ait kişisel verileri çaldı ve tüm veriyi Dark Web üzerinde 20.000 dolar değerindeki bitcoin karşılığında sattı.
- Avustralya'da 15 bin hastanın medikal kayıtları ele geçirildi.
- ABD'nin Connecticut eyaletinde 326 bin hastanın e-postaları ihlal edildi.
- Washington eyaletindeki neredeyse 1 milyon hastanın verilerini içeren sunucu ifşa edildi.
- 2,7 milyon İsveç vatandaşının sağlık raporları internete sızdırıldı.
- Facebook ve Instagram yüz milyonlarca kullanıcısının verileri internete sızdırıldı. Korunmasız sunucularda yer alan 540 milyon adet data (kullanıcı adı, kimlik bilgisi ve şifre) ortalığa saçıldı.
- ABD'de 2002-2010 yılları arasında görülmüş sayısız davaya ait olan çoğu gizli 250 bin yasal belgenin yer aldığı sunucunun siber suçlular tarafından ele geçirildi.
- Hindistan'da devlete bağlı bir kurumdaki 12,5 milyon hamile kadına ait medikal kaydın siber suçluların eline geçtiği kaydedildi.
- Gayrimenkul firması First American Financial şirketine ait yüz milyonlarca sigorta belgesi internete sızdı.
- San Francisco Körfezi bölgesinde faaliyet gösteren iki rakip firmadan Choicelunch'ın baş finans yöneticisi, rakibi theLunchMaster'ın web sayfasına siber saldırı düzenlemek suçundan tutuklandı. Saldırıda, birçok öğrenciye ait verilerin ele geçirildiği anlaşıldı.

2019 yılından Siber Saldırı Örnekleri – 2

- Amerikan Medikal Veri Toplama Derneği'nin (AMCA) sunucularında bulunan en az 20 milyon hasta bilgisi ele geçirildi. Müşterilerin ödeme bilgilerinden sosyal güvenlik numaralarına, medikal verilerinden doğum tarihlerine ve hatta telefon numaraları ve adreslerine kadar sayısız kritik bilgi siber suçluların eline geçti. Sonuçta, AMCA sayısız dava ile karşılaştı ve bu yükü kaldıramayarak iflasını açıkladı.
- Capital One yaşanan güvenlik bariyeri ihlali ile 100 milyon kredi kartı uygulamasına ait veri kaptırdı. Siber suçlular 140 bin sosyal güvenlik numarası, 80 bin banka hesap numarası ve adreslerden telefon numaralarına ve doğum tarihlerine kadar kişisel verileri ele geçirdi. Veri kaybının ardından Capital One, FBI soruşturması altına alındı. Soruşturmada, saldırının arkasında bilişim uzmanı (IT) çalışanından hacker'a dönüşen Paige A. Thompson adlı kişinin olduğu anlaşıldı.
- İndirimli sinema biletleri ile cazip teklifler sunan MoviePass, 160 milyondan fazla müşteri verisini şirket sunucularında şifresiz olarak sakladığını fark etti.
- İngiltere'de Metropolitan Police departmanı, çeşitli bankalar ve şirketlerin sunucularında tutulan 27,8 milyon biyometrik kayıt, siber suçluların eline geçti.
- Words with Friends oyununa ait 218 milyondan fazla oyuncu verisi internete sızdırıldı. E-posta adresleri, isimler, kayıt bilgileri gibi hassas veriler, son derece basit bir saldırı ile kaybedilmişti. Bir hacker, önemli bir güncelleme öncesinde oyunda hesap açan kişileri hedefleyerek güvenlik önlemlerini kolayca aştı.
- 17,5 milyon nüfuslu Ekvador'da hükümete ait sunuculardaki 20,8 milyon kişinin verilerinin çalınması oldu. Doğum tarihi, ulusal kimlik numaraları, adresler, telefon numaraları ve eğitim bilgileri gibi her türlü şahsi bilgi Dark Web'e düştü.
- Adobe'nin korunmasız bıraktığı sunucusundaki 7,5 milyon Creative Cloud müşteri bilgisi ele geçirildi.
- Rusya'da ise 20 milyon vatandaşın vergi bilgilerinin korunmasız bırakıldığı ve 2009-2016 arasındaki vergi bilgilerinin çoktan buhar olduğu ortaya çıktı.
- Trend Micro firmasında bir "içten saldırı" vakası ortaya çıkarıldı. Şirketin müşterilerine ait 70 bin veriyi ele geçiren bir çalışan, bu verilerle müşterileri dolandırdığı anlaşıldıktan sonra tutuklandı.
- Hollandalı bir politikacı ve şehir konseyi üyesinin yıllardır internet üzerinden kadınlara şantaj yapan bir hacker olduğu ortaya çıktı. 2014'te tespit edilen ve Hollywood ünlüleri dahil sosyal medyada tanınan kişilerin çıplak fotoğraflarını çalan bir gruba üye olduğu düşünülen politikacı, Hollanda'da 100 kadının iCloud hesaplarına sızarak özel fotoğraflarını çaldı. YouTube ünlülerinden sporculara kadar 100 kadına şantaj hazırlığında olan politikacı, 3 yıl hapis cezası istemiyle yargılanıyor.
- Türkiye'de bir banka ağır bir DDOS saldırısına maruz kaldı ve birkaç saat tüm işlemleri durdurmak zorunda kaldı.
- Türkiye'de bir Telekom firması siber saldırıya uğradı ve yüksek miktarda müşteri datası ihlali yaşandı.

Teşekkürler!

volkan@birsensigorta.com