EY Türkiye
Siber Güvenlik Bülteni

COVID-19 Salgını ile ilgili Siber Riskler ve operasyonel güvenlik ve sürdürebilirliği sağlamak adına öneriler

23 Mart 2020

Building a better working world

Coronavirus'ün yayılmasıyla dünyada 1 milyonun üzerinde organizasyon etkilenecek[1]. En fazla etkilenen ülkeler ise global ekonominin yaklaşık %40'ını temsil ediyor[2].

Farklı sektörlerdeki işletmeler, salgından kaynaklanan etkiler nedeni ile gelişen bir siber tehdit ortamı ile karşı karşıya olabilir.

- Buna ilave olarak aniden uzaktan çalışma modeline geçildiğinden, yeni risklerin anlaşılması ve bunlara ilişkin aksiyon geliştirilmesi siber güvenlik uzmanları üzerinde ekstra yük ve baskı oluşturmaktadır.

"

Yönetim Kurulu üyelerinin **79%'u** organizasyonlarının bir krize yeteri kadar hazır olmadığını düşünüyor..[3]

COVID-19 salgını ortasında Çekya'da hastaneye siber saldırı!

ZDNet

Forbes

Coronavirus Alarmı: COVID-19 temalı web sitelerine ve e-postalara dikkat.

Coronavirus temalı domain'ler (alan adları) diğerlerine göre %50 daha fazla zararlı yazılım riski taşıyor.

CheckPoint

RedDrip Team

Ukrayna Sağlık Bakanlığı'na bağlı Halk Sağlığı Merkezi'nden geliyormuş gibi gelen saldırılar oltalama için dokümanlar kullanıyor!

1: CNBC, 4 Şubat
2: McKinsey
3: Global Risk Survey 2020

Farklı sektörlerdeki işletmeler, salgından kaynaklanan etkiler nedeni ile gelişen bir siber tehdit ortamı ile karşı karşıya olabilir.

Uzaktan çalışmadaki artış yeni riskler doğuruyor

Güvenlik yerine erişilebilirliği tercih eden yaklaşımlar

Yönetilmeyen yazılım/varlıklar

Onaylanmış uzaktan çalışma yazılımlarından memnun olmayan veya kullanma zorluğu çeken kullanıcıların kendi uygulamalarını yüklemelerine veya "gölge BT" kurmalarına yol açabilir.

Yama ertelemeleri

Uzaktan çalışmaya imkan veren kaynaklara olan yüksek talep, yama için gereken sistem kapama / durdurma sürelerine imkan tanımayabilir.

Ağ "düzleşmesi« (flattening)

Kurum bütününde kaynaklara bağlantı sağlama çabası ağ ayrıştırmasını riske atabilir.

Daha önceden yüz yüze olan aktivite ve işlemlerin dağılması

Ağ güvenliğinde değişiklikler

Uzaktan gerçekleştirilen yüksek düzeyli işlemler alarmları tetikleyebilir. Yeni durum tanımlanana kadar tüm trafik anomali olarak görünebilir.

Yardım masası ve BT'de iş yükü

- Uzaktan çalışan kullanıcılar kimlik doğrulama / yetkilendirme süreçlerini atlatacak şekilde yardım masasını talep yağmuruna tutabilir.
- BT hizmetleri için gerekli olan fiziksel varlıklar erişilemez hale gelebilir.
- Üçüncü taraf riskleri aynı kısıtlamalarla ortaya çıkabilir.

Mevcut tehditler belirsizlik ve kamu ilgisinden faydalanıyor

Tehdit vektörleri, taktikleri ve hedefleme stratejileri

Oltalama, zararlı siteler, & iş e-posta mesajlarını ele geçirme

Sahte haber güncellemeleri, ihtiyati yönlendirme, virüs haritaları, tahlil sonuçları veya çalışan bilgi notları hedef olabilir.

Para sızdırma, yıkıcı/yok edici saldırılar ve markaya zarar

- Salgın ile ilgili baskı altında olduğu hissedilen kuruluşlar hedef alınabilir.
- Uygunsuz olduğu kabul edilen eylemler veya ifadeler "hacktivist"leri ya da içeriden tehditleri tetikleyebilir.

Tehdit aktörü motivasyonları, araçları ve hedefleri

Profesyonel suçlular & görece yeni gelenler

- **Araçlar:** İndiriciler, tuş kaydediciler, oltalama siteleri, fidye yazılımları, uzaktan erişim araçları.
- **Hedefler:** Hassas sağlık bilgileri, kişisel veriler, erişim bilgileri, bağışlar ve fidyeler.

Devlet destekli gruplar

- **Araçlar:** İndiriciler, tuş kaydediciler, uzaktan erişim eklentileri, casus yazılımlar.
- **Hedefler:** Sürekli casusluk; virüsle ilgili sağlık bilgisi toplama.

Bu tehdit ve risklere karşı işletmeler farklı unsurları olan risk azaltıcı faaliyetleri düşünebilir.

VPN, ağ cihazları ve uzaktan çalışmayı mümkün kılan cihazların **güncel yama ve güvenlik konfigürasyonlarına** sahip olunmasına adına güncellemeler yapın.

Tüm VPN bağlantılarında 2+ Faktörlü Kimlk Doğrulama (Multi Factor Authentication - **MFA)** kullanın. Bu mümkün değilse uzaktan çalışan personelin **güçlü parolalar** kullandığından emin olun.

VPN kapasitesinin BT güvenlik ekiplerince test edildiğinden emin olun. Mümkünse daha fazla bant genişliğine ihtiyacı olan çalışanlara bu imkanı verebilmek adına kısıtlamalara ilişkin politikalar oluşturun.

Yüksek yetkili erişimlerin düzenli olarak izlendiğinden emin olun. Mümkünse sistem yöneticisi (admin) seviyesindeki kullanılacıların ay da hassas veriye erişimi olan personelin olası şüpheli işlemlerini tespit etmen adına davranışsal analitik araçlar kullanın.

Log izleme ve alarm takibi açısından **Security Information and Event Management (SIEM)** sistemleri kullanın. **Güvenlik Operasyon Merkezi (Security Operation Center SOC)** ve izleme ekiplerinin yüksek sayıda alarm takibi, bunların risk analizleri ve false-pozitive kayıtların ayrıştırılması için ihtiyaç duyabilecekleri efor artışına karşı personel planlaması yapın.

Log gözden geçirme, saldırı tespit, olay müdahale ve kurtarma gibi siber güvenlik faaliyetlerine daha fazla önem gösterin.

Çalışanlarınıza artabilecek **oltalama saldırıyla** ilgili uyarın. Özellikle **Coronavirüs ile ilgili web siteleri ve e-postalar** gibi zararlı yazılım ihtiva etmesi muhtemelen ortamlara girmeden BT ve güvenlik ekiplerine bilgi vermelerini sağlayacak yönlendirme, bildirim ve duyuruları yapın.

Web ve e-posta güvenliği için filtreleme teknolojileri kullanın, bunlardan kaynaklı riskleri azaltmak adına özelleştirilmiş kuralları devreye sokun. Özellikle bir hastane ya da kritik altyapıya sahip kurumda çalışıyorsanız daha sıkı kuralları ve güncel beyaz listeleri kullanmayı gündeme alın.

Yönetici (admin) erişim ve faaliyetlerini zorlaştırın. Gerçekten ihtiyaç duyulan faaliyetleri listeleyin, kuralları bunlara göre sıkılaştırın.

Acil durum ve kriz yönetimi yetkinliklerinizi güncelleyin, buna göre **kaynak tahsislerini** yeniden değerlendirin. **Sistem ve veri yedeklerinizi** kontrol edin, çalıştıklarından emin olun. **Yardım Masası** personelinin karşılamak zorunda kalacağı talep ve çağrılarının artacağını öngörerek bunlara ilişkin prosedürlerinizi gözden geçirin.

Son kullanıcı güvenliğini ihmal etmeyin, mümkünse ilave kuralları devreye alın.

En kötü senaryoları düşünün, kriz yönetimi ve olay müdahale planlarınızı ve kritk tedarikçilerinizin erişilebilirlik durumlarını buna göre yeniden değerlendirin.

Çalışanlarınıza vermeniz gereken mesajlar.

Uzaktan çalışmak için kullanılan ofis ekipmanlarının diğer hane halkı tarafından kullanımına izin vermeyin. Kişisel bir cihaz üzerinden iş yapmak gerekirse antivirüs vb. güvenlik önlemlerinin alındığından emin olun.

Kurum politika ve prosedürlerini takip edin, bunlara uyun. Online güvenliğiniz için şüpheli e-postaları açmayın, web sitesi linklerine tıklamayın.

Salgın ile ilgili güncel bilgiler için resmi kaynakları takip edin, hijyen kurallarına uyun.

İletişim Bilgileri

Emre Beşli

EY Türkiye Şirket Ortağı

Risk Danışmanlığı Hizmetleri Bölüm Başkanı

Emre.Besli@tr.ey.com

Ümit Yalçın Şen

EY Türkiye Şirket Ortağı

Siber Güvenlik Hizmetleri Lideri

Umit.Sen@tr.ey.com