Kriz Anında Kurumunuzun Siber Güvenliğini Sağlayın

COVID-19 salgınının potansiyel siber güvenlik etkilerini anlama ve yönetme

COVID-19 ’a Yönelik Tedbirler:

Siber Güvenlik

İnsanların yaşamları, aileleri ve içinde bulundukları toplum üzerinde büyük etkilere neden olan COVID-19 salgını, Dünya Sağlık Örgütü tarafından “pandemi” ilan edildi

Krizlerde ve öngörülemeyen olaylarda işletmeler önemli zorluklarla ve yavaşlamalarla karşı karşıya iken **yolunu bulma yeteneği,** operasyonel esnekliğin önemli bir ayağıdır; özellikle bir halk sağlığı krizi durumunda.

Belirsiz zamanlarda iş faaliyetlerini sürdürmek için, işletmelerin **siber saldırılara, artan uzaktan çalışma taleplerine ve gittikçe karmaşıklaşan yönetim süreçlerine yanıt vermek** için bütünsel bir yaklaşım sergilemesi ve bunu prova etmesi gerekir.

pwc

Kültür ve Farkındalık

Siber risklerin arttığı dönemde son kullanıcı davranışı ve kurum kültürü

Yönetişim

Olağan dışı durumlarda güvenlik postürünü korumak için etkili bir yönetişim yürütme

Veri Güvenliği

Farklı çalışma pratiklerini uygularken ve kullanırken hassas bilgileri koruma

Kapasite Yönetimi

Uzaktan çalışma ve güvenli veri erişimi sağlamak için gerekli kritik güvenlik hizmetlerine yönelik artan talebi yönetme

Tespit edici ve Önleyici Kontroller

Olağan dışı durumlarda dahi iş süreçleri üzerindeki izleme, algılama ve koruma kontrollerini sürdürme

Vaka Yönetimi ve İş Sürekliliği

Organizasyonel stresin arttığı bir dönemde vaka yönetimi, kriz ortamına müdahale ve iş sürekliliği yetkinliklerini işletmeye devam etme

Ne zaman harekete geçilecek?

Aşamalı Müdahale Planı - COVID-19

Sınırlama	Geciktirme	Araştırma	Hafifletme
Vakalar mümkün mertebe erken tespit edilmeli, yakın temaslar takip edilerek hastalığın kök salmasını geciktirmek için önlemler alınmalı.	Alınan önlemlerle hastalığın yayılım hızı ve yüzeyi takip edilerek gerekli ek önlemler ile yavaşlatılmalı.	Virüsün nüfus üzerindeki etkisini azaltacak eylemler daha iyi anlaşılmalı; teşhis, ilaçlar ve aşılar dahil olmak üzere yenilikçi yanıtlar bulunmalı; kanıtlar bakım modellerinin gelişimine katkı sağlamak için kullanılmalı.	Hasta olan insanlar için mümkün olan en iyi bakım sağlanmalı, hastaneler temel hizmetleri sürdürebilmeleri için desteklenmeli ve toplumda hasta olan insanlar için hastalığın toplum, kamu hizmetleri ve ekonomi üzerindeki genel etkisini en aza indirmek için sürekli destek sağlanmalı.

Hazırlık	Müdahale	İyileşme
Harekete geç Kuruluşlar yıkıcı bir olayın içindeyken siber risklere yönelik daha yüksek bir hazırlık durumuna geçmeli, bu noktada siber kriz yönetimi ve iş sürekliliği planlarını yürürlüğe koymalıdır. Bu dönemde, siber risklerin dinamik olarak değerlendirilmesine ihtiyaç duyulacaktır.	**Yeni gelişmelere dinamik olarak müdahale et** Organizasyonlar, kriz yönetimi ve iş sürekliliği planlarının uygulandığı değişken bir ortamda faaliyet göstereceklerdir. Bu sebeple artan iş riskleri bağlamında, kuruluşlar giderek daha çevik bir işletim modeline geçmeye öncelik vermelidir. Bu dönem, potansiyel olarak yeni teknolojilerin hızlı bir şekilde konuşlandırılmasını ve üçüncü taraf uzman desteğinin alınmasını gerektirebilir. Özellikle, kuruluşların ticari operasyonlarını bu belirsizlik ortamında sürdürebilmeleri için, uzaktan çalışma talepleri gibi normalin dışına çıkan ihtiyaçlara yanıt verebilecek bir altyapı oluşturmaları gerekebilir.	**Normal düzene geri dönüş ve öğrenilen dersler** İşletmeler olağan operasyonlarına kriz yönetimi prosedürlerini aşamalı olarak kaldırarak dönmelidir. İyileştirme alanlarını belirlemek ve planlarını buna göre güncellemek için öğrenilen dersler dikkate alınmalıdır (Örneğin; güvenlik operasyonlarını giderek otomatikleştirmek gibi seçenekleri dikkate almak ve eksiklikleri tespit etmek).

Hazırlık

COVID-19 Siber Müdahale Stratejisi

Çalışanlar

Çalışanlarınızın alternatif çalışma pratiklerine geçiş yapabilir olmasını sağlayın

- Tüm kullanıcılar uzaktan çalışma metodu için kendilerine sunulan teknolojilerin ve süreçlerin farkında mı?
- Kurumunuz, farklı çalışma yöntemleri sunarken değişen duruma ve şartlara göre önem kazanabilecek siber risklerin farkında mı? Bir değerlendirme yapıldı mı? (Örneğin; uzaktan çalışırken veri güvenliğinin sağlanması)
- Kurumunuz, alternatif çalışma uygulamalarına geçerken, yeni ortamı destekleyecek yeterli yetkinlikte ve sayıda güvenlik uzmanlığına (kurum içi ve üçüncü taraf) sahip mi?
- Güvenli uzaktan çalışma ve güvenli veri işlemeyi destekleyecek iyi uygulamaları yönetmek için, kurumunuz politikalar ve süreçler oluşturdu mu? Bunlar daha geniş iş alanlarınıza (iştirakler, 3. taraflar) iletildi mi?
- Güvenlik Operasyon Merkeziniz (SOC) veya bu hizmeti sağlayan ekibiniz, daha yüksek bir siber güvenlik esnekliğine (24x7 hizmet verecek şekilde veya vardiya modeline geçmek gibi) uyum sağlamaya hazır mı?
- Üst düzey yöneticileriniz, bir siber olay olması durumunda güvenlik iletişim protokollerinin farkında mı?

Süreç

Veri güvenliğini arttırmak ve siber risklere hazır olmak için kurumunuzla işbirliği içinde çalışın

- Uzaktan çalışırken hassas verilerin güvenli bir şekilde işlenmesi için belirlenmiş ve anlaşılmış süreçler var mı?
- Uzaktan çalışma için rehber oluşturulup kuruluş içinde gerekli taraflara iletildi mi? Kolay erişilebilir bir ortamda mı?
- Kurumun güvenlik prosedürlerinin geçici personel / acil durum personeli tarafından uygulanması için bilgi aktarım mekanizmaları oluşturuldu mu?
- Güvenlik eğitimi ve farkındalık materyallerinin yeni gelişmelere uygun olarak dinamik bir şekilde güncellenmesi için süreçler mevcut mu?
- Olası artış gösterecek uyarılara yanıt vermek için siber güvenlik ekiplerinin kapsam genişletme, kaynak arttırma süreçleri uygulanabilir durumda mı?
- Standart güvenlik süreçleri uzaktan çalışan personel için uygulanabilir olmaya devam edecek mi (Örneğin; Virüs tarama, loglama ve yama güncellemeleri)?
- Standart güvenlik faliyetleri nasıl devam edecek, belirlendi mi (Örneğin; güvenlik açığı değerlendirmeleri)?

Teknoloji

Yeterli kapasiteyi sağlamak için mevcut teknolojiyi gözden geçirin gerekliyse güncelleyin

- Tüm uç nokta aygıtları için uzaktan erişim ve VPN uygulamalarınız var mı?
- Uzaktan erişim ve VPN uygulamalarınız taleplere bağlı olarak ölçeklenebilir mi?
- VPN uygulamalarınızda çok faktörlü kimlik doğrulaması uygulanıyor mu?
- Uzaktan erişen kullanıcılar için kimlik yönetimini nasıl yönetiyorsunuz?
- Kullanıcılar sistemlere uzaktan eriştiğinde kullanıcı gözetimini nasıl sağlıyorsunuz?
- Ağ üzerinde gelişmiş kontrol sağlamak için ek güvenlik kontrolleri uyguluyor musunuz? (Örneğin; Sanal ağ bölgelemesi, uç nokta cihaz uyum kontrolü vb.)
- Güvenlik izleme kurallarınız sizi şüpheli / olağandışı VPN etkinliği konusunda uyarıyor mu?
- Ağ bant genişliği, uzaktan erişim hizmetlerinin kullanımını destekleyecek mi yoksa yoğunluk nedeniyle hizmet kesintisi yaşanabilir mi?

Müdahale

COVID-19 Siber Müdahale Stratejisi

Çalışanlar

Çalışanlarınızın olağan dışı çalışma ortamlarında iş yapabilmesi için gerekli desteği almasını sağlayın

- Operasyonlarınız önemli bağımlılıkları ve tek noktaya bağımlılık ilkesini gözetecek şekilde değerlendirildi mi?
- Eğitimler ve rehber materyaller, çalışanların; uzaktan çalışma düzeni ve veri güvenliğini sağlama ilkelerine uymaları için hazır ve erişilebilir durumda mı?
- Çalışanlar, kişisel cihazları ile şirket kaynaklarına /uygulamalarına erişim konusunda uymaları gereken güvenlik tedbirleri hakkında bilgilendirildi mi?
- Uzaktan çalışma süresi boyunca güvenlik soruşturmalarını incelemek için atanan bir görevli bulunuyor mu?
- Çalışanlar olası güvenlik vakalarının nasıl raporlanması gerektiği konusunda bilgilendirildi mi?
- Raporlama süreciyle ilgili bilgiler, merkezi bir ortamda ilgili kullanıcıların erişimine açık mı?
- Kullanıcılara güvenli bir haberleşme aracı sağlanıyor mu ve kullanıcılar bu aracı nasıl kullanacağını biliyor mu?
- Güvenlik ekibinin bir mensubunun rahatsızlanması durumu göz önünde bulundurarak alternatifler yöntemler düşünüldü mü? (takımlara ayrılma, ofis ziyaretlerinin azaltılması vs.)

Süreç

Güncel süreçleri yeni çalışma prensiplerine adapte edin

- Bildirim/ raporlama prosedürleri, uzaktan çalışma süreçlerini destekleyecek şekilde gözden geçirilip güncellendi mi?
- Kriz döneminde dışarıdan çalışma süreçleri ve yöntemlerinin etkililiği nasıl ölçülecek?
- Yeni gelişmeler ışığında eğitim materyallerinin devamlı güncellenmesi ve yayılması için bir süreç belirlendi mi?
- Destek ekiplerinin siber güvenlik olaylarına nasıl müdahale edeceğini gösteren iş akışları veya süreçler erişilebilir durumda mı?
- Kritik güvenlik süreçleri, değişen çalışma uygulamalarına göre nasıl adapte oluyor?
- Kritik güvenlik süreçleri (erişim yetkilerinin incelenmesi, DLP karantinası gibi) gerektiği gibi çalışıyor mu?
- Üçüncü kişilerle iletişimin nasıl yapılacağı hakkında açık ve güncel bir plan var mı, özellikle kritik iş süreçleri ve konumları işleten kişiler için (veri merkezleri gibi)
- Zafiyet ve yama yönetimi gibi standart süreçler, kriz döneminde nasıl yürütülür belirlendi mi?
- Değişiklik yönetiminde olası bir durdurma (freeze) gündeme gelirse, kritik zafiyetlerin/ güncelleme ihtiyaçlarının ortaya çıkması durumunda bu değişikliklerin nasıl yapılacağı değerlendirildi mi?

Teknoloji

Teknolojik altyapıda iyileştirmeler yaparak değişen taleplere yanıt verebilir olun

- Şirketin güvenlik yapısı, hızlı gelişen gereksinimleri karşılamak için kısa bir zaman zarfında geliştirilebilecek durumda mı?
- Eğer ek güvenlik servislerine ihtiyaç olursa, halihazırdaki güvenlik seviyesi esnetilmeden bu servisler nasıl adapte edilir?
- Kullanıcıların uzaktan bağlantı yapmaları durumunda hassas/kritik sistemlere erişimlerini kısıtlayabilecek veya sınırlandırabilecek bir erişim yönetimi çözümü var mı? (spesifik bir cihaz ile erişim sağlama gibi)
- Veri merkezleri, iş sürekliliğini sağlamak için ağ yükünü dengeleyecek/ karşılayacak altyapı düzenine ve kapasiteye sahip mi?
- Yeni ortamda şirket ağındaki sıra dışı kullanıcı davranışlarını saptayıp inceleyecek bir güvenlik politikası ve çözümü belirlenmiş durumda mı?
- Kısa bir zaman süresinde kullanıcı bilgilerini inceleyecek, güncelleyecek ve yenileyecek güvenlik sistemleri mevcut mu? (acil durum erişim belirleme gibi)
- Eğer AI/ otomatik tespit etme sistemleri yürürlükteyse, bu sistemler yeni çalışma koşullarına göre nasıl adapte edildi?
- Kritik fonksiyonların devamlılığı için, geçici olarak devre dışı bırakılabilecek güvenlik servisleri olabileceği seçeneği değerlendirildi mi?

İyileşme

COVID-19 Siber Müdahale Stratejisi

Çalışanlar

Çalışanlarınızın normal çalışma koşullarına dönüşünü sağlayın

- Kurum kriz dönemi süresince, uzaktan çalışma aktivitelerini devamlı olarak izleyebildi mi? Uygun olmayan, şüpheli son kullanıcı aktiviteleri tespit edilebildi mi? IK bu durumda nasıl davranacağını belirledi mi?
- Kriz dönemi boyunca standart yönetim prosedürlerinde değişiklikler ya da esnemeler yapıldıysa tekrar normal iş akışına dönülmesini sağlanacak müdahaleler yapıldı mı?
- Standart iş süreçlerine dönülmesini sağlamak için faydalı güvenlik yöntemlerini göz önünde bulunduran iletişim yolları belirlendi mi? (güvenli veri arşivi gibi)
- Öğrenilen dersler nasıl tespit edilecek ve kullanıma alınacak izlenecek yol belli mi?
- Kriz döneminde hangi güvenlik adımlarında farklılıklar oluştu tespit edildi mi? Bu tespitler gelecekteki kültür farkındalığına nasıl katkı sağlayacak?
- Kriz boyunca kurumun güvenlik kültürü esnetilmeden uygulanabildi mi? Yoksa kullanıcıların zor durumlarda kaldığı ve esneklik talep ettiği durumlar yaşandı mı?

Süreç

Öğrenilen dersleri ve planlarınızı tekrar gözden geçirerek güncelleyin

- Kriz dönemi süresince operasyon ve yönetim modelinde sık yaşanan/tekrarlayabilen hataları giderecek bir acil durum planı geliştirildi mi? (kritik personele bağımlılık, fazla yetki kullanımı, onay sürecinin kaldırılması gibi)
- Öğrenilen güvenlik noktaları, özellikle güvenliğin etkilediği iş operasyonlarına nasıl etki etti? Bu etkilerin ışığında daha geniş bir iş sürekliliği planı geliştirildi mi?
- Kaynak tüketimi yoğun olan güvenlik süreçleri otomatikleştirilebilecek süreçleri saptama amacıyla gözden geçirildi mi?
- Standart dışı ortamda çalışırken tespit edilen zafiyetler, problem sonrasında güvenlik testlerine tabi tutuldu mu?
- Gelecekte benzer kötü senaryoların yaşanmasına karşılık, işlerin sekteye uğramasını minimize etmek için yeni iş süreçleri tasarlandı mı?
- Güvenlik risklerinin transferi gibi kontrol mekanizmalarının işleri nasıl iyileştirebilecekleri yönünde araştırma yapıldı mı? (siber sigorta gibi)

Teknoloji

Operasyonel çevikliği artırmak için teknolojik seçenekleri göz önünde bulundurun

- İş faaliyetlerini personel yetersizliği dönemlerinde sürdürmek için otomatik güvenlik yönetimi seçenekleri gözden geçirildi mi (Örneğin; otomatize edilmiş algılama ve koruma çözümleri)?
- Hizmetlerin uzun vadede isteğe bağlı ölçeklenebilirliğini arttırmak için bulut tabanlı çözümler değerlendirildi mi?
- Üçüncü taraf hizmet sözleşmeleri, beklenmedik durumları içerecek veya düzeltecek şekilde yeniden değerlendirildi mi?
- Kişisel cihazlardaki işlevselliği genişletmek amacıyla mobil cihaz yönetimi çözümleri değerlendirildi mi?
- Gelecekte güvenlik mimarinizin daha dayanıklı veya çevik olabilmesi için nasıl değişmesi gerekiyor, çözümleri değerlendirdiniz mi?
- İşletmelerin dayanıklılığı ve esnekliği yönetebilme kabiliyetini gelişen teknolojiler nasıl daha iyi hale getirebilir? Bu teknolojilerin güvenlik ortamına etkisi ne olur? (Örneğin; arttırılmış gerçeklik, dronlar)?

2020-0078