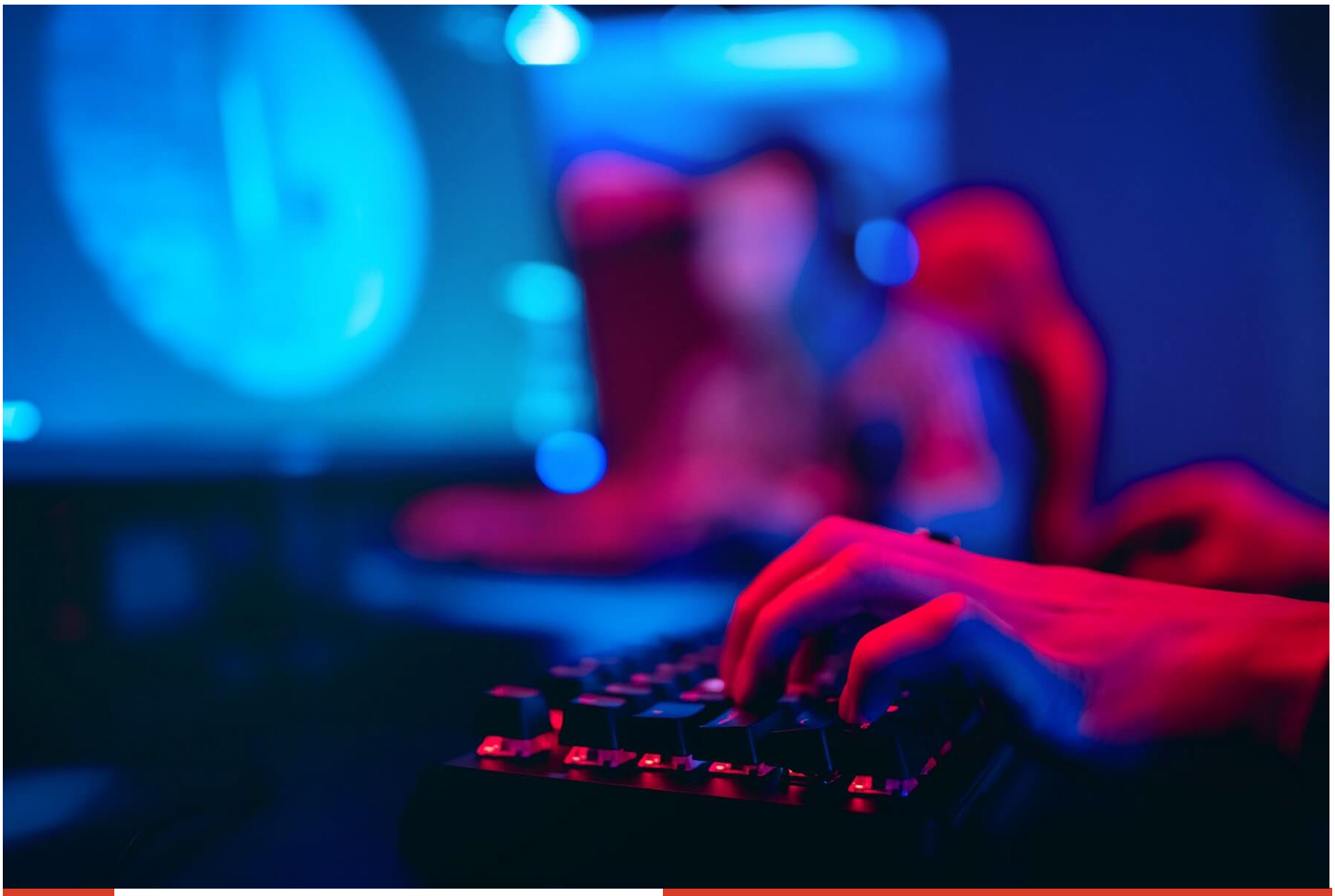
OLAY MÜDAHALE REFERANS REHBERİ

YASIN KARAMAN, IT BUSINESS MANAGEMENT (B.SC. – PROFESSIONAL), CISSP, CEH

ONUR SAVAŞ, PENETRATION TESTER



Önce, Zarar Vermeyin

Tıbbın kritik bir ilkesi siber güvenlik olaylarına müdahale için de aynı derecede geçerlidir - Zarar Vermeyin.

Kuruluşlar, bir olayın olumsuz etkisini önemli ölçüde artırabilecek birçok tuzakla karşı karşıyadır.

Bu kılavuz, yaygın hatalardan kaçınarak bir siber güvenlik olayını yönetmenize yardımcı olmak ve olay müdahale çabalarınızın hem etkinliğini hem de verimliliğini artırmak için tasarlanmıştır.

Olay Müdahale Referans Kılavuzu

Siber Güvenlik Olayları için İlk Yardım

İÇİNDEKİLER

ANAHTAR ÇIKARIMLAR

Hazırlık işe yarar - Büyük bir olaya hazırlıklı olmak, kuruluşa verilen zararı azaltmanın yanı sıra olay maliyetini ve yönetim zorluğunu da azaltabilir.

Olay yönetimi süreçlerinizi operasyonel hale getirin - Siber güvenlik olaylarını yönetmek, standart iş riski yönetimi süreçlerinin bir parçası olmalıdır.

Koordinasyon kritiktir - Etkili siber güvenlik olay yönetimi teknik, operasyon, iletişim, hukuk ve yönetişim fonksiyonlarının işbirliği ve koordinasyonunu gerektirir.

Sakin olun ve bir olayda zarar vermeyin - Aşırı tepki vermek, yetersiz tepki vermek kadar zarar verici olabilir.

GENEL BAKIŞ

Ne yazık ki çoğu kuruluş, bir saldırganın iş süreçlerinizi sağlayan ve kritik iş verilerinizi depolayan BT sistemleri üzerinde idari kontrole sahip olduğu bir veya daha fazla büyük olay yaşayabilir.

Bu, siber güvenlik konusunda size yardımcı olacak "ilk yardım" tarzı bir rehberdir:

1. **Krize Hazırlanın** - Temel hazırlıklarla kuruluşunuzun riskini azaltın.

2. **Bir Kriz Durumunda** - Kuruluşunuza gelebilecek olası zararı derhal sınırlandırın.

Bu, büyük bir siber güvenlik olayının teknik, operasyonel, yasal ve iletişim yönleri için ipuçları ve rehberlik içerir.

Bu üst düzey ipuçları ve uygulamalar bir krizin yönetilmesinde değerli olsa da, her olay benzersiz ve karmaşıktır.

Bu ilk yardım kiti eksiksiz bir müdahale ve kurtarma kılavuzu sağlamak üzere tasarlanmamıştır. Bu belgede açık ya da zımni hiçbir garanti bulunmamaktadır. Kapsamlı rehberlik ve uzman tavsiyesi için aşağıdakileri tavsiye ederiz:

- Aktif bir büyük olay için profesyonel yardım almayı düşünmelisiniz.

- Ek hazırlık kılavuzu için NIST Özel Yayını 800-184 "Siber Güvenlik Olay Kurtarma Kılavuzu "nu incelemelisiniz http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

HEDEF KITLE

Bu kılavuz öncelikle Bilgi Güvenliği Direktörü (CISO), Baş Hukuk Müşaviri, İletişim/PR Lideri ve Bilgi Teknolojileri Direktörü (CIO) rolündeki kişiler ve yakın çalışma arkadaşlarına yöneliktir, ancak diğer birçok rol ve paydaş da bu bilgileri değerli bulacaktır.

GIRIŞ

Birçok kuruluş büyük bir olayla karşılaşacak veya müşterilerden, ortaklardan ve yönetim kurulundan gelen bir siber güvenlik saldırısını önleme, tespit etme ve başarılı bir şekilde yönetme konusundaki zor sorulara yanıt vermek zorunda kalacaktır.

2016-2017 EY anketi, yönetim kurulu üyelerinin ve C-suite üyelerinin %87'sinin kurumlarının siber güvenlik düzeyine güvenmediğini göstermiştir. Bu belge, bu zorlukları daha iyi yönetmenize yardımcı olmak için tasarlanmıştır ve, çeşitli şirketler ve devlet kurumlarındaki kolektif deneyimlerimize dayanmaktadır.

Son zamanlarda siber güvenlik tehditlerinde yaşanan artış ve bunlara karşı savunma yapmanın zorluğu göz önüne alındığında, kuruluşlar güvenlik yatırımlarından en fazla getiriyi nasıl elde edeceklerine odaklanmalıdır. En büyük güvenlik yatırım getirisi, güvenlik çabalarınıza ve bütçenize öncelik vermenizden kaynaklanacaktır. Saldırganın maliyeti, fırsatçı tehditleri caydıracağı ve kararlı düşmanları yavaşlatacağı (veya ideal olarak durduracağı) için.

İyi planlanmış bir müdahaleye hazırlanmak ve bunu uygulamak, saldırganların operasyonel maliyetini artırabilir ve büyük bir siber güvenlik olayının kuruluşunuz üzerindeki iş etkisini önemli ölçüde azaltabilir.

Siber Güvenlik Olayları

Güvenlik olayı, kurumdaki bilgi kaynaklarının ve varlıklarının gizliliğini, bütünlüğünü veya kullanılabilirliğini etkileyen bir olaydır. Bir olay düşük etkiden, kurumsal BT sistemlerine idari erişimin tehlikeye girdiği büyük bir olaya kadar değişebilir (basında sıkça yer alan hedefli saldırılarda olduğu gibi).

Bir güvenlik olayı genellikle hassas bilgilerin ihlaliyle sonuçlanır, ancak bazen bunun yerine operasyonel/veri imhasıyla sonuçlanır. Kişisel bilgi ihlalinin birçok yargı alanında özel yasal gereklilikleri vardır.

Bu tür olayların üstesinden gelmek, büyük bir kriz operasyonunu yönetmek için gerekli donanıma veya eğitime sahip olmayan kuruluşlar için çok zor olabilir.

Ekiplerimiz, mevcut felaket kurtarma planları/tatbikatları ile entegre olan ve Olay Komuta Sistemi (ICS) gibi kriz yönetimi mekanizmalarını kullanan kuruluşların büyük bir siber güvenlik olayını yönetme konusunda önemli ölçüde daha iyi deneyimler edindiğini gözlemlemiştir.

Bu kılavuz öncelikle NIST siber güvenlik çerçevesinde tanımlanan Müdahale ve Kurtarma aşamalarına odaklanmaktadır. Büyük olayların önlenmesi ve tespit edilmesine ilişkin rehberlik için bkz. http://aka.ms/SPAroadmap

Hazırlık

"Şans, hazırlıklı zihinden yanadır."

Louis Pasteur

Hazırlık

Bu bölüm, bu temel işlevler genelinde kurumsal ihlal müdahale planınızı oluşturmanın veya güncellemenin temel yönlerini düşünmenize ve planlamanıza yardımcı olmak için tasarlanmıştır:

- Teknoloji
- Operasyonlar
- Yasal
- İletişim

Birçok kuruluşun siber saldırılarla ilgili felaketlerle karşılaşma olasılığı yangın, deprem veya sel felaketleriyle karşılaşma olasılığından daha yüksektir.

Bir siber güvenlik saldırısına yanıt vermek için iyi bir hazırlık, aşağıdaki riskleri önemli ölçüde azaltabilir.

Bu bölümde, deneyimlere dayalı olarak, bir siber güvenlik saldırısına yanıt vermede en büyük etkiye sahip hazırlık unsurları sunulmaktadır.

Teknoloji

Büyük bir siber güvenlik olayına müdahale ve kurtarma hazırlığı, bir olaya karşı korunma, olayı tespit etme ve olaya müdahale etme adımlarını içermelidir.

Koruma ve Algılama hazırlığı için, http://aka.ms/sparoadmap adresindeki büyük olaylarda kullanılan yaygın saldırı yöntemlerine odaklanan teknik denetimlerin Microsoft ayrıcalıklı erişimi güvence altına alma (SPA) yol haritasını izlemenizi öneririz.

Yanıt vermeye hazırlanmak için aşağıdakileri öneriyoruz.

GENEL HAZIRLIKLAR

Yüksek Değerli Varlıkları (HVA - High value assets**) belirleyin** - Kritik öneme sahip iş varlıklarını ve bunların teknik bileşimini (sunucular, uygulamalar, veri dosyaları vb.) belirlemeniz gerekir. HVA bileşenlerinin bu envanteri, kurtarma planlarının bu kritik varlıkları hızla değerlendirmesi, kontrol altına alması/izole etmesi ve kurtarması için kritik öneme sahiptir.

Güvenilir Yazılım Dağıtımını Onaylayın - Tüm uç noktalarda komut dosyalarını/yükleyicileri hızla çalıştırabileceğinizi doğrulayın. Deneyimlerimize göre, eksik veya güvenilir olmayan yazılım dağıtım sistemleri kurtarma çabalarını önemli ölçüde engelleyebilir.

SORUŞTURMA HAZIRLIKLARI

Tehdit algılama ve izleme yetenekleri - Ortamınızdaki gelişmiş saldırganları tespit etmenize olanak tanıyan araçlara ve becerilere erişiminiz olduğunu doğrulayın. Bu yetenekler sürekli olarak gelişmektedir, ancak şu anda gelişmiş bir program şunları içerir:

- Olay korelasyonu ve analizi
- Entegre tehdit istihbaratı
- Kullanıcı ve Varlık Davranış Analitiği
- Hem geçmiş kalıplar için Uzlaşma Göstergeleri hem de gelişen teknikler için Saldırı Göstergeleri ile tespit etme yeteneği
- Makine öğrenimi analitiği

En kritik temel tespit yetenekleri SPA yol haritasında (yukarıda) özellikle belirtilmiştir.

Soruşturma ve Adli yetenekler - Kapsamlı bir saldırı zaman çizelgesi oluşturabilen kötü amaçlı yazılım analizi ve saldırı etkinliği analizini içeren hedefli saldırıları araştırmak için gelişmiş araçlara ve becerilere erişiminiz olduğunu doğrulayın. Bu yeteneklere erişim sağlayabilirsiniz. Araçları satın alarak ve analistleri işe alarak veya harici kuruluşlar veya profesyonel hizmetler aracılığıyla erişimi koruyabilirsiniz.

Müdahale maliyetlerini takip ve analiz edin - Daha iyi risk yönetimi sağlamak için, olaya müdahale etmekle ilgili maliyetlerin kaydını tutmalısınız. Bu, hem doğrudan maliyetleri (harici hizmetler, müşteriler için kredi raporlaması vb.) hem de ekibinizin soruşturma ve kurtarma için harcadığı zamanın maliyetinin yanı sıra kuruluşunuzun işi ve misyonu üzerindeki olumsuz etkiyi de içermelidir.

KURTARMA HAZIRLIKLARI

Kritik veriler için doğrulanmış yedekleme ve kurtarma özelliği - Örneğin, verileri silen veya şifreleyen (fidye yazılımı gibi) yıkıcı bir saldırıya hazırlanmak, çevrimdışı ve/veya fidye yazılımına dayanıklı bir yedekleme özelliği (Microsoft Azure Backup gibi) kullanarak kritik verileri kurtarma yeteneğinizi doğrulamanızı gerektirir.

Teknik dokümantasyon/otomasyon oluşturma - Bir güvenlik olayı sırasında sıklıkla gerekli olan prosedürler için teknik dokümantasyon (ve/veya otomasyon) yazın ve doğrulayın:

Aşağıdakilerin dikkate alınmasını içeren ele geçirilmiş hesap kurtarma prosedürleri

- Hesabın ele geçirilmesine ilişkin güven düzeyleri (aktif saldırgan kullanımı, ele geçirildiği bilinen ana bilgisayarda açığa çıkan hesap kimlik bilgileri, şüpheli hesap davranışı, vb.

- Çevrimdışı yedeklemeler, değişiklik günlükleri veya diğer kayıt sistemleri kullanılarak hesaplara müdahale edilip edilmediği nasıl doğrulanır?

- Şifrenin sıfırlanması veya hesabın hızla yeniden oluşturulması

- Herhangi bir hesabın yeniden oluşturulması sırasında Kimlik Yönetimi sistemiyle olası çakışmaların/entegrasyonun nasıl ele alınacağı

Hem iş istasyonları hem de sunucular için tehlikeye atılmış ana bilgisayar kurtarma prosedürleri. Bu şunları içermelidir:

- Ana bilgisayar işletim sistemi (ve uygulama) yeniden oluşturma prosedürleri

- Temizleme prosedürleri ve ne zaman temizlenip ne zaman yeniden inşa edileceğine ilişkin kriterler (eğer kuruluşunuzda bir ana bilgisayarın "temizlenmesi" kabul edilebilir görülüyorsa)

- Aşağıdakileri yapabilme becerisi de dahil olmak üzere ağ ayrıştırma ve izolasyon prosedürleri

- Saldırgan Komuta ve Kontrol (C2) kanalları için internet çıkış noktası günlüklerini arayın ve izleyin

- İnternet çıkış noktalarında saldırgan C2 kanallarını engelleyin

- Mümkünse, yüksek değerli varlıkları üretim ortamındaki diğer uç noktalardan (güvenliği ihlal edilmiş iş istasyonları ve sunucular gibi) izole edin

Ağ ayrıştırma ve izolasyon prosedürleri de dahil olmak üzere:

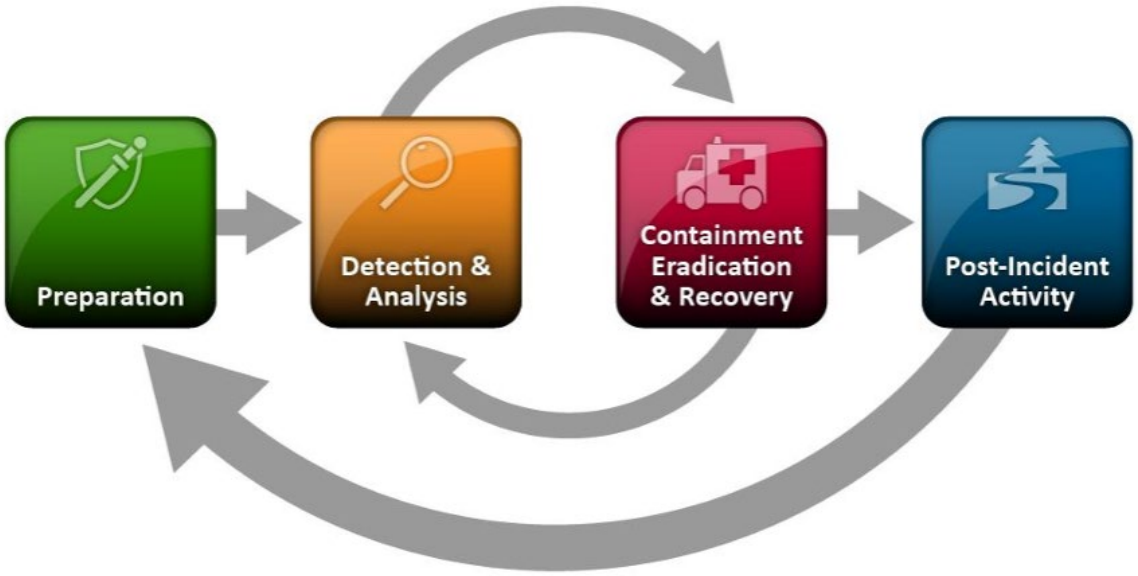
- Saldırgan Komuta ve Kontrol (C2) kanalları için internet çıkış noktası günlüklerini arayın ve izleyin
- İnternet çıkış noktalarında saldırgan C2 kanallarını engelleyin
- Mümkünse HVA'ları üretim ortamındaki diğer uç noktalardan (güvenliği ihlal edilmiş iş istasyonları ve sunucular gibi) izole edin

Operasyonlar

Bir siber güvenlik olayını yönetmek teknik karmaşıklıklar, bilinmeyen değişkenler ve yüksek duygularla dolu zorlu bir olaydır. Çünkü İş faaliyetleriniz üzerindeki potansiyel ciddi etki, çabaları, kaynakları ve zamanı aşağıdakileri gerçekleştirmeye yönlendirmek için net bir iş vakası oluşturulabilir. Bir siber olay sırasında bir işletme olarak hayatta kalmak için gerekli planlama ve hazırlık.

Yakın zamanda yapılan EY GISS anketinde, kurumların %57'si iş sürekliliği yönetimini (BCM) veri sızıntısı/veri kaybının önlenmesi ile birlikte en önemli öncelikleri olarak değerlendirmiştir.

ABD NIST, hazırlık ihtiyacını vurgulayan birçok önemli hususu içeren faydalı bir belge yayınlamıştır:

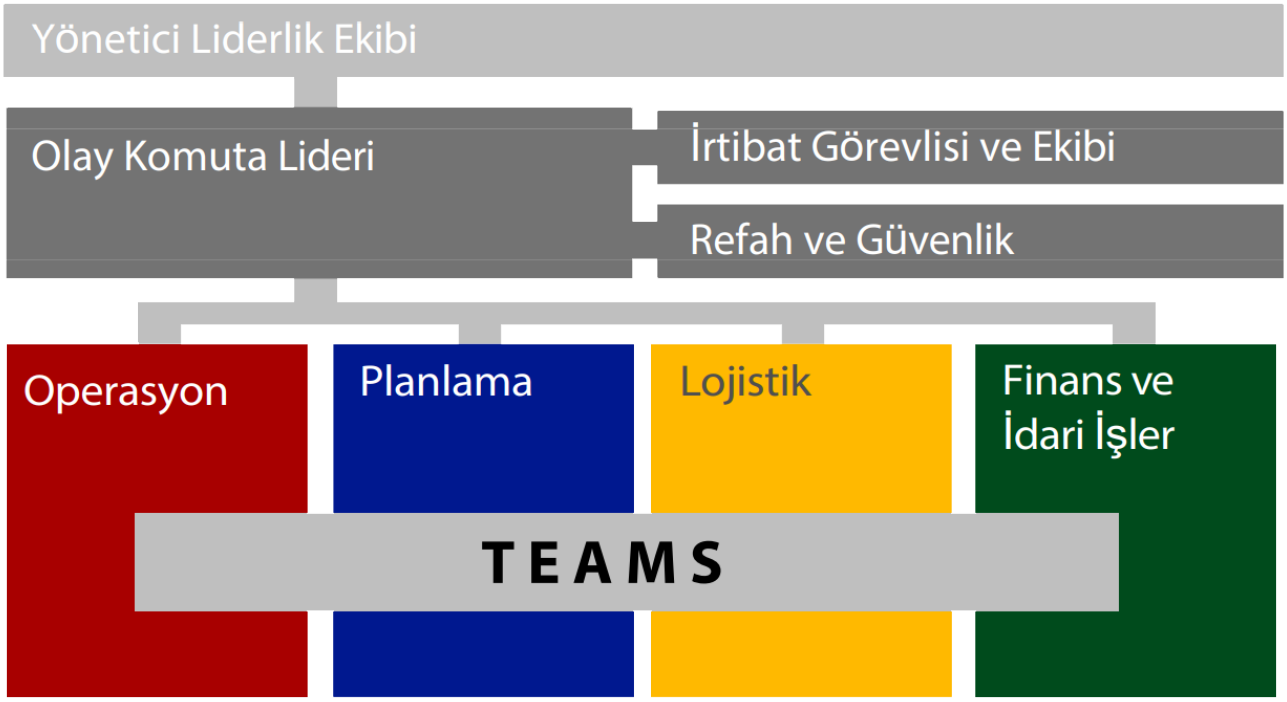


Bu bölüm, operasyonlar için öğrenilenleri ve önerilen uygulamaları paylaşarak kurumsal riski azaltmaya yardımcı olmak üzere tasarlanmıştır.

KRİTİK HAZIRLIKLAR

Kriz Yönetimi için Olay Komuta Sistemini (ICS) benimseyin - Büyük olaylar kurumsal bir krizi temsil eder ve bunları yönetmek için geçici bir komuta yapısı gerektirir (bunun için zaten kalıcı bir işleviniz yoksa). ICS doğal afetlerde yaygın olarak kullanılmaktadır ve birçok siber güvenlik olayında son derece değerli olduğunu kanıtlamıştır.

https://en.wikipedia.org/wiki/Incident_Command_System



Bir Çerçeve Oluşturun - Olay müdahale programınızı tanımlayan bir çerçeveniz olduğunu teyit edin.

Kriz Sürecinizi Tatbik Edin - Kriz ekiplerini ve süreçlerini tüm sorumluluk seviyelerinde ilgili senaryolar üzerinde tatbik etmek için yinelenen bir program oluşturun. Bu program bireysel bileşenlerin tatbikatlarını ve tüm paydaşları (hukuk, iletişim ve kurumsal liderlik dahil) içeren masa başı tatbikatları içermelidir. Ayrıca bu tatbikatlar sırasında yedekleme kurtarma ve tehdit tespit araçları dahil olmak üzere müdahaleci olmayan teknik prosedürleri de doğrulamalısınız.

Acil Durum Onay Süreci - Acil durum/olay sırasında hızlı değişiklikleri ele almak için kolaylaştırılmış bir acil durum onay süreciniz olduğunu teyit edin (örneğin, hızlı değişiklik tekliflerini değerlendirme/onaylama yetkisi ve sonrasında süreç boyunca değişiklikleri ve geri bildirimleri yakalamak için hükümler).

Eskalasyon için Net Yönergeler Belirleyin - Dahili soruşturmaların ne zaman uzmanlara ve harici soruşturma ekiplerine yükselmesi gerektiğine dair eşikleri belgeleyin. Bunlar harcanan zamana, karmaşıklığa, bilinmeyen kötü amaçlı yazılımlara, belirli bir düşmana vb. dayalı olabilir.

GÜÇLÜ BIR MÜDAHALE PROGRAMININ AYIRT EDICI ÖZELLIKLERI

Modern kuruluşların karmaşıklığı nedeniyle, ideal müdahale programı sektörden sektöre ve kuruluştan kuruluşa değişecektir. Güçlü bir olay müdahale ve kurtarma programının genel özellikleri şunlardır:

Güçlü bir şekilde entegre edilmiştir:

- İş öncelikleri ve liderlik
- BT Operasyonları
- İş Sürekliliği Yönetimi ve Felaket Kurtarma
- İç ve dış kaynaklardan gelen bağlam

Sürekli öğrenme kültürü ve süreçleri:

- Ölüm sonrası incelemeler yapıldı ve çıkarılan dersler entegre edildi
- Düzenli tatbikatlar ve kırmızı ekip doğrulaması

Dokümantasyon:

- Tüm paydaşlar tarafından müdahale çerçevesine yüksek düzeyde aşinalık
- BT ve Güvenlik Uzmanları için ayrıntılı teknik kurtarma talimatları (veya otomasyon)

Büyük olaylar için Teknik Hazırlık:

- Güvenlik sistemleri ve kritik iş sistemleri ile ilgili teknik yeterliliğe erişim
- Güvenlik olaylarının operasyonel, iletişim ve yasal yönleri konusunda deneyime erişim (dahili ekipler ve/veya harici kuruluşlarla ortaklıklar / hizmet alımı yoluyla)

ÇIKARILAN KILIT DERSLER

Gözlemlediğimiz daha güçlü programlar bu temel dersleri öğrenmiştir:

- Sadece daha fazla araç satın almak daha iyi güvenlik anlamına gelmez.
- Kullanacak zaman ve beceriye sahip olmadan araç satın almak israf ve dikkat dağıtıcıdır.
- Her günlük kaynağını (Loglar) etkinleştirmek sizi yalnızca veriye boğacak, daha fazla iğne bulmak yerine samanlığın boyutunu artıracaktır.
- Güvenlik personelinizi BT operasyonları ile ikili bir role yerleştirmek, onların etkinliğini azaltır.
- Personelinizi hazırlayarak ve gerekli kaynakların kullanılabilirliğini planlayarak bir olayın maliyetini azaltabilirsiniz.
- Aynı saldırganları ve teknikleri tekrar tekrar göreceğiniz için öğrenilen dersleri yakalamak başarı için kritik önem taşır.

KURUMSAL HAZIRLIK ÖZ DEĞERLENDİRMESİ

Bu sorular, kuruluşunuzun büyük bir olayı yönetmeye ne kadar hazır olduğunu belirlemenize yardımcı olacaktır.

TEMEL STRATEJİ VE UYUM

- HVA'larınızı (süreçler, veriler, donanım, kimlikler) iyi anlıyor musunuz?
- HVA'larınız ve en olası saldırı yolları için gelişmiş kontrolleriniz var mı?
- Yüksek olasılıklı saldırı vektörleriniz nelerdir? Saldırganların ilk erişimi elde etmek ve ardından kalıcılık veya daha yüksek erişim seviyeleri elde etmek için ikincil saldırı seviyelerini denemeye başlamak için hangi saldırgan tekniklerini kullanma olasılığı en yüksektir?
- Hazırlık için yatırım yapmazsanız iş kaynaklarınız ve itibarınız üzerindeki etkisini ölçebilir misiniz?

GÜVENLİK OPERASYONLARI

Çogu kurunmlar tehdit istihbarat programına sahip değildir ya da sadece gayri resmi bir programa sahiptir. Mobil cihazlarla ilgili zayıf kullanıcı farkındalığı ve davranışı konusunda endişe duymaktadır.

- Siber tehditleri tespit etmeye ve bunlara yanıt vermeye odaklanmış bir güvenlik operasyon merkeziniz var mı?

- Bilinen tehditleri ele almak için belirlenmiş bir güvenlik ekibiniz ve müdahale iş akışlarınız var mı?

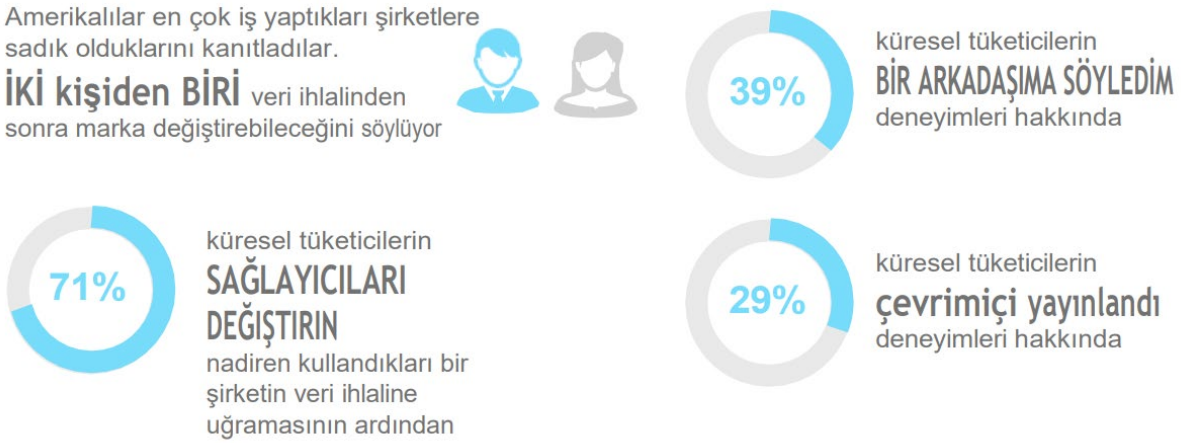
- Olaylara müdahale için belgelenmiş, sosyalleştirilmiş ve uygulanmış bir süreciniz var mı?

- Çalışanlarınıza siber tehditleri araştırmaları için uygun eğitim ve zaman veriliyor mu?

- Araçlarınız siber tehditleri tespit etmede ne kadar etkili?

İletişim

Bir güvenlik olayının yönetilmesiyle ilgili tüm büyük maliyetler ve riskler arasında, marka ve itibara gelebilecek potansiyel darbe ve müşteri güveninin kaybı en zarar verici olabilir. Edelman'ın güvenlik araştırmasına göre, küresel tüketicilerin %71'i nadiren kullandıkları bir şirketin veri ihlaline uğraması durumunda sağlayıcılarını değiştireceklerini söylemiştir. İtibar etkisinin ötesinde, kötü yönetilen ve iletilen güvenlik olayları çalışanların moralini etkileyebilir ve düzenleyici baskı ve davalara yol açabilir.



Siber saldırılar arttıkça beklentiler de değişiyor. Kuruluşlardan güvenlik olaylarını mutlaka önlemeleri beklenmiyor (bu riskin niteliğine bağlı olsa da), ancak bir siber saldırının sonuçlarını etkili bir şekilde yönetmeleri bekleniyor. Bu konuda giderek artan bir fikir birliği vardır. Son derece sofistike siber savunma sistemleri bir saldırıya kurban gidebilir ve şirketler bir olayın meydana gelmesini önleyip önleyemediklerinden ziyade bir olayı ne kadar iyi yönettiklerine göre değerlendirilmelidir.

Güvenlik olaylarıyla ilgili etkili iletişim kurmak, dikkatli bir planlamanın yanı sıra siber güvenlik sorunlarını diğer kriz türlerinden farklı kılan benzersiz dinamiklerin anlaşılmasını gerektirir. Şeffaflık ve hızın genellikle doğru hareket tarzı olduğu geleneksel kriz konularının aksine, adli tıp incelemelerinin karmaşık doğası gerçekleri akışkan hale getirdiği için ilk bulguların ve ayrıntıların iletilmesinde büyük risk vardır. Bu dinamik, daha sonra yanlış olduğu ortaya çıkan bilgilerin müdahale sürecinin başlarında ifşa edilme potansiyelinin artmasına yol açar. Bu durum güvenilirlik kaybına, ek haber döngülerine ve olumsuz haberlerin artmasına yol açabilir.

Aşağıda, kuruluşların olası bir olayla başa çıkmaya hazırlıklı olmak için şimdiden atmayı düşünmeleri gereken birkaç adım yer almaktadır.

BIR OLAYDAN ÖNCE

- Temel olay müdahale ekibinin bir parçası olacak bir iletişim sorumlusu atayın ve bu kişinin müdahale sürecini ve siber güvenliği anladığını teyit edin. Bir kriz anında, iletişimi kimin yöneteceğini ve bir kurum adına kimin konuşacağını belirlemek için değerli zaman ve enerji harcanır. Siber güvenlik olaylarının ve soruşturmalarının iletişiminde güçlü bir iletişim liderinin etkili olmak için anlaması gereken benzersiz nüanslar vardır. Bu kişinin çekirdek ekibin bir parçası olması, iletişim ve itibar yönetiminin karar alma sürecinde uygun şekilde temsil edilmesini sağlayacaktır.

- Açık sahiplik ve onay süreçleri de dahil olmak üzere mevcut olay müdahale planlarının iletişim bölümünü geliştirin. Birçok şirket, bir sorunun nasıl araştırılacağını ve düzeltileceğini özetleyen teknik olay müdahale planlarına sahiptir. Genellikle eksik olan, neyin kime ve ne zaman açıklanacağına karar vermenin karmaşık hesabını yönetmek için iletişim merkezli bir bölümdür.

- Müşteriler, medya, ortaklar, düzenleyiciler, çalışanlar ve satıcılar dahil olmak üzere bir olayla ilgili iletişim alması gerekebilecek paydaşların haritasını çıkarın. Bu, şirketin belirli ortakları veya müşterileri bilgilendirmek için sözleşmeden doğan yükümlülüklerini anladığını teyit etmeyi de içerir. Olaylar genellikle düzenleyicilere veya tüketicilere açıklama yapılmasını gerektirmeyebilir, ancak yine de kurumsal müşterilerle zamanında paylaşılmaları gerekir. Bir olay öncesinde bu yükümlülüklerin anlaşılması, canlı bir olay sırasında değerli zaman kazandırabilir.

- Şirketinizi en çok ilgilendiren başlıca olay türleri için taslak medya holding açıklamaları ve diğer materyalleri geliştirin. Bu açıklamaların, soruşturmanın ilk aşamalarında, konunun pek çok ayrıntısı henüz bilinmezken basınla birlikte kullanılması amaçlanmaktadır. Her bir olay için, bir olay meydana geldiğinde karar verme sürecine yardımcı olabilecek temel iletişim hususlarını geliştirmek de önemlidir. Örneğin, şirketin fidye yazılımını kaldırmak için ödeme yapıp yapmayacağı ve hangi koşullar altında ödeme yapacağı ve bu kararı kilit paydaşlara nasıl konumlandıracağı.

- Bir olay nedeniyle medyanın, müşterilerin ve düzenleyici kurumların ilgisine nasıl tepki vereceklerini test etmek için tüm olay müdahale ekibinden üyelerle bir masa başı tatbikatı düzenleyin. Bu masa başı tatbikatlar genellikle en iyi şekilde dış hukuk müşaviriyle birlikte yapılır ve olay müdahalesinin teknik olmayan tüm yönlerine odaklanmayı amaçlamaz.

Yasal

Hukuk müşavirliği, proaktif siber güvenlik programı geliştirme, uygulama ve yürütmede giderek daha kritik bir rol oynamaktadır. Tüm uyumluluk rejimlerinde olduğu gibi, siber güvenlik avukatları da yasal, sözleşmesel ve düzenleyici görevlere ilişkin hukuki tavsiyelerin yanı sıra denetimler, soruşturmalar veya davalardan kaynaklanabilecek yasal risklerin yönetilmesi ve azaltılması konusunda tavsiyelerde bulunur. Deneyimli düzenleyiciler artık kuruluşların bir olaya hazırlanmasını ve düzenleyici yaptırım kararlarını bu mercekten değerlendirmesini beklemektedir.

Aşağıda, siber güvenlik alanında proaktif yasal iş akışlarının bazı temel yönleri yer almaktadır:

- **Hukuk departmanından bir Siber Lider atayın.** Siber güvenlik olaylarına müdahale hazırlıklarının büyük bir kısmı yasal risklerin değerlendirilmesini ve yönetilmesini içerir. Hukuk müşavirleri (dahili ve/veya harici) belirli olay müdahale hazırlık faaliyetlerini "yönlendirecek" ve proaktif ve reaktif çalışmalarının avukat-müvekkil ayrıcalığı kapsamında olma olasılığını en üst düzeye çıkarmak için dışarıdan adli tıp ve iletişim uzmanları tutacak şekilde konumlandırılmalıdır.

- **Politikaları ve Kamu Açıklamalarını Gözden Geçirin.** Yaptığınızı söylüyorsanız, yapsanız iyi olur. Bu sadece kamuya açık beyanlar (örneğin gizlilik beyanları, hizmet beyanları) için değil, aynı zamanda dahili güvenlik politikaları için de geçerlidir. Bu politikalar ve kamuya yapılan açıklamalar, mevcut durumu temsil edecek şekilde düzenli olarak gözden geçirilmeli ve gereksiz yere büyük veya kesin ifadelerden kaçınılmalıdır. Bir şirketin siber güvenlik programı hakkındaki ifadeler (örneğin, "banka düzeyinde güvenliğimiz var" veya "son teknoloji siber güvenliğimiz var").

- **Bir Olay Müdahale Planı geliştirin.** Olay Müdahale Planı, bir şirketin bir güvenlik tehlikesi veya veri ihlaline vereceği yanıtın farklı yönlerini bir araya getiren temel operasyonel belgedir. Düzenleyiciler ve davacılar yalnızca teknik güvenlik önlemlerine değil, aynı zamanda bir siber saldırıyla karşılaşıldığında şirketin verdiği yanıtın hızına, verimliliğine ve etkinliğine de odaklanır. Uzman siber danışmanlar, düzenleyici kurumlardan ve dava konusu olaylardan elde edilen en son bilgileri yansıtan operasyonel açıdan etkili süreçler oluştururken, bir yandan da kasıtsız sorumluluk kabullerinden veya ne makul ne de ulaşılabilir olan geçici standartlar oluşturmaktan kaçınarak özenli bir anlatı oluşturmayı amaçlar.

- **Hukuk Departmanının Talimatıyla Siber Güvenlik Değerlendirmeleri ve Testleri Yapın**. Bu değerlendirmelerden elde edilen sonuçlar, düzenleyiciler ve davacılar tarafından ilk talep edilenler arasındadır. Kuruluşlar genellikle bu değerlendirmelerden çıkan tüm önerileri uygulayamadığından, ekipler iyileştirme ve azaltma çabaları konusunda riske dayalı kararlar vermelidir. Hukuk müşavirleri (içeriden veya dışarıdan) sızma testleri, güvenlik açığı değerlendirmeleri vb. yapmak üzere siber güvenlik danışmanları tutmalı ve çalışmalarını BT Güvenliği ile çok yakın işbirliği içinde kapsamlandırmalı ve yönlendirmeli, böylece ilgili iletişimleri, iş ürünlerini ve müzakereleri yasal ayrıcalık altında korumalıdır.

Raporlar, keşif risklerini en aza indirmek için az miktarda ve yalnızca avukatın talimatı üzerine hazırlanmalıdır.

- **Düzenli Yönetim Kurulu Bilgilendirmeleri Yapın.** Yönetim kurulu üyeleri risklerin farkında olmadıkları takdirde güvene dayalı sorumluluklarını yerine getiremezler. Buna göre, yönetim kurulları siber güvenlik riskleri hakkında düzenli olarak bilgilendirilmeli ve siber güvenlik riskini etkin bir şekilde yönetebilmeleri için siber güvenlik riskini anlama ve değerlendirme konusunda yeterli bilgi ve uzman yardımı sağlanmalıdır.

- **Üçüncü Taraf Satıcıları Yönetin.** Kurumsal ağa veya müşteriler/çalışanlar hakkındaki kişisel verilere erişimi olan üçüncü taraflar saldırı yüzeyini genişletir ve genellikle "en zayıf halkayı" temsil eder. Özen gösterme aşamasında, satıcılar sundukları risklere göre değerlendirilmelidir. Anlaşmalar, satıcıların uyması gereken güvenlik standartlarını; satıcıların nasıl araştırma yapacakları, işbirliği yapacakları ve ilgili kişileri bilgilendirecekleri konusunda net bir süreci ve bir olay meydana geldiğinde yasal korumaları (tazminat, sorumluluğun sınırlandırılması, sigorta vb.) içerecek şekilde müzakere edilmelidir. Son olarak, kuruluşlar tedarikçilerin güvenlik standartlarına uyumunu test etmek için bir denetim, inceleme veya sertifikasyon süreci geliştirmelidir.

Bir kriz anında

"Gelecek hafta bir kriz olamaz. Programım zaten dolu."

Henry Kissinger

BIR OLAY SIRASINDA, ŞUNLARI YAPMAK ÇOK ÖNEMLIDIR:

- **Sakin olun** - Olaylar son derece yıkıcıdır ve duygu yüklü hale gelebilir. Sakin olun ve çabalarınızı öncelikle en etkili eylemler üzerinde yoğunlaştırmaya odaklanın.

- **Zarar vermeyin** - Müdahalenizin veri kaybını, iş açısından kritik işlevsellik kaybını ve kayıpları önleyecek şekilde tasarlandığını ve yürütüldüğünü teyit edin. Kaçınılan kararlar, adli zaman çizelgeleri oluşturma, temel nedeni belirleme ve kritik dersler çıkarma becerinize zarar verebilir.

- **Doğru Olun** - Kamuoyu ve müşterilerle paylaştığınız her şeyin doğru ve gerçek olduğunu teyit edin.

- **Gerektiğinde yardım alın** - Sofistike saldırganlardan gelen saldırıları araştırmak ve bunlara yanıt vermek, derin uzmanlık ve deneyimden önemli ölçüde yararlanır.

Tıbbi hastalıkların teşhis ve tedavisinde olduğu gibi, büyük bir olay için siber güvenlik araştırması ve müdahalesi, her ikisi de olan bir sistemi savunmayı gerektirir:

- Kritik derecede önemli (üzerinde çalışmak için kapatılamaz)

- Karmaşık (tipik olarak herhangi bir kişinin kavrayabileceğinin ötesinde)

Bir olay sırasında birkaç kritik dengeyi sağlamanız gerekir

- **Hız:** Paydaşları memnun etmek için hızlı hareket etme ihtiyacı ile acele karar verme riskini dengelemelisiniz.

- **Bilgi paylaşımı:** Sorumluluğu ve gerçekçi olmayan beklentileri sınırlandırırken müfettişleri, paydaşları ve müşterileri bilgilendirmelisiniz.

Bu bölüm, kaçınılması gereken yaygın hataları belirleyerek ve hem riski azaltan hem de paydaşların ihtiyaçlarını karşılayan hangi eylemleri hızla gerçekleştirebileceğiniz konusunda rehberlik sağlayarak bir olayda işletmenizin karşılaşacağı riski azaltmak için tasarlanmıştır.

Teknoloji - Araştırma Aşaması

KRİTİK BAŞARI FAKTÖRLERİ

- **Saldırı operasyonunun kapsamını belirlemelidir** - Çoğu düşman birden fazla kalıcılık mekanizması kullanır.

- Kalıcı saldırganlar gelecekteki bir saldırıda sıklıkla hedefleri (veriler/sistemler) için geri döneceklerinden, mümkünse saldırı hedefini belirleyin.

İPUÇLARI

- **Dosyaları çevrimiçi ortama yüklemeyin** - Birçok saldırgan, hedeflenen kötü amaçlı yazılımların keşfi için VirusTotal gibi hizmetlere güvenen örnekleri izler.

- **Değişiklik yok** - İş açısından kritik verileri kaybetme (silme, şifreleme, dışarı sızma) gibi yakın bir tehditle karşılaşmadığınız sürece, soruşturma tamamlanana kadar kurtarma işlemlerine başlamayın.

- **Sonsuza kadar araştırma yapmayın** - Araştırma çabalarınızı acımasızca önceliklendirmelisiniz (örneğin, yalnızca saldırganların gerçekten kullandığı veya değiştirdiği ana bilgisayarlar üzerinde adli analiz gerçekleştirin). Bir saldırganın yönetici ayrıcalıklarına sahip olduğu büyük bir olayda, potansiyel olarak tehlikeye atılmış tüm kaynakları (tüm kurumsal kaynakları içerebilir) araştırmak pratik olarak imkansızdır.

- **Bilgi paylaşımı** - Tüm soruşturma ekiplerinin (tüm dahili ekipler ve harici soruşturmacılar dahil) verilerini birbirleriyle tam olarak paylaştıklarını teyit edin.

- **Doğru Uzmanlığa Erişin** - Sadece güvenlik genel uzmanlarını değil, sistemler hakkında derin bilgiye sahip kişileri (gerektiğinde dahili personel veya satıcılar gibi harici kuruluşlar) soruşturmaya entegre ettiğinizden emin olun.

- **Yasal kontrol** - Soruşturma ve kurtarma prosedürlerini uygun şekilde planlayabilmeniz için hukuk departmanınızla kolluk kuvvetlerini dahil etmeyi planlayıp planlamadıklarını kontrol edin.

- **Müdahale kabiliyetiniz olumsuz etkilenecektir** - Durumsal stres nedeniyle personelinizin %50'sinin normal kapasitenin %50'sinde çalışmasını planlayın.

Teknoloji - İyileşme Aşaması

KRİTİK BAŞARI FAKTÖRLERİ

Okyanusu kaynatmayın - Müdahale kapsamını kurtarma işleminin 24 saat veya daha kısa sürede gerçekleştirilebileceğini doğrulayacak şekilde sınırlandırın (beklenmedik durumları ve düzeltici eylemleri hesaba katmak için bir hafta sonu planlayın).

- **Dikkat dağıtıcı unsurlardan kaçının** - Büyük/karmaşık yeni güvenlik sistemlerinin uygulanması gibi uzun vadeli güvenlik yatırımlarını erteleyin veya kurtarma işleminden sonraya kadar kötü amaçlı yazılımdan koruma çözümlerini değiştirmeyin. Mevcut kurtarma operasyonu üzerinde doğrudan ve acil bir etkisi olmayan her şey dikkat dağıtıcıdır.

İPUÇLARI

- **Asla tüm parolaları bir kerede sıfırlamayın** - Parola sıfırlamaları öncelikle güvenliği ihlal edildiği bilinen hesaplara ve potansiyel olarak yönetici/hizmet hesaplarına odaklanmalıdır. Gerekirse, kullanıcı parolaları yalnızca aşamalı/kontrollü bir şekilde sıfırlanmalıdır.

- **Kurtarma görevlerinin yürütülmesini birleştirin** - İş açısından kritik verileri kaybetme gibi yakın bir tehditle karşı karşıya değilseniz, tehlikeye atılmış tüm kaynakları (ana bilgisayarlar, hesaplar vb.) hızlı bir şekilde düzeltmek için birleştirilmiş bir operasyon planlamalısınız. Bu zaman aralığını sıkıştırmak, saldırı operatörlerinin uyum sağlamasını ve kalıcılığını sürdürmesini zorlaştıracaktır.

- **Mevcut Araçları Kullanın** - Kurtarma sırasında yeni bir aracı dağıtmaya ve öğrenmeye çalışmadan önce halihazırda dağıttığınız araçların (yazılım dağıtımı, kötü amaçlı yazılımdan koruma vb.) yeteneklerini araştırın ve kullanın.

- **Düşmanlara bilgi vermekten kaçının** - Mümkün olduğunca, kurtarma operasyonu hakkında düşmanların ulaşabileceği bilgileri sınırlandırmak için adımlar atmalısınız. Düşmanlar genellikle büyük bir siber güvenlik olayında tüm üretim verilerine ve e-postalara erişebilir, ancak gerçekte çoğu saldırganın tüm iletişimlerinizi izleyecek zamanı yoktur. Gerektiğinde, olay müdahale ekibinin üyeleri için güvenli işbirliği için üretim dışı bir Office 365 kullanın.

Operasyonlar - Soruşturma Aşaması

KRİTİK BAŞARI FAKTÖRLERI

- **Odaklanın** - İş açısından kritik verilere, müşteri etkisine ve iyileştirmeye hazır olmaya odaklandığınızı teyit edin.
- **Koordinasyon ve rol netliği** - Kriz ekibini destekleyen operasyonlar için farklı roller belirleyin ve teknik, hukuki ve iletişim ekiplerinin birbirlerini bilgilendirdiklerini teyit edin.
- **İş perspektifi** - Hem düşman eylemlerinin hem de müdahale eylemlerinizin iş operasyonları üzerindeki etkisini her zaman göz önünde bulundurmalısınız.

İPUÇLARI

- **Kriz yönetimi için ICS'yi düşünün** - Güvenlik olaylarını yöneten kalıcı bir organizasyonunuz yoksa, ICS'yi krizle başa çıkmak için geçici bir organizasyon yapısı olarak kullanmanızı öneririz.
- **Gösteri devam etmeli** - Olay incelemelerini desteklemek için günlük güvenlik operasyonlarının tamamen bir kenara bırakılmadığını teyit edin. Normal işlerin hala yapılması gerekmektedir.
- **Savurgan harcamalardan kaçının** - Birçok büyük olay, kuruluşların panik içinde hiçbir zaman konuşlandırılmayan veya kullanılmayan bir dizi pahalı güvenlik aracı satın almasıyla sonuçlanır. Soruşturma sırasında bir aracı konuşlandıramayacak ve kullanamayacaksanız, satın almayı soruşturma bitene kadar erteleyin. Ayrıca, aracı çalıştırmak veya araçtan değer elde etmek için gereken nadir veya özel beceri setleri için insanları işe alma/eğitme/koruma yeteneğinizi de göz önünde bulundurun.
- **Derin uzmanlığa erişim** - Soru ve sorunları kritik platformlardaki derin uzmanlara iletme becerisine sahip olduğunuzu onaylayın. Bu, iş açısından kritik sistemler ve kurumsal çapta bileşenler (masaüstü bilgisayarlar, sunucular vb.) için işletim sistemi ve uygulama satıcısına erişim gerektirebilir.

Operasyonlar - İyileşme Aşaması

KRİTİK BAŞARI FAKTÖRLERI

- **Net Plan ve Sınırlı Kapsam** - Teknik ekiplerle yakın çalışarak Sınırlı kapsamı olan net bir plan üzerinde çalışılmalı. Planlar düşman faaliyetlerine veya yeni bilgilere göre değişebilirken, ek görevlerin "kapsam genişlemesini" sınırlamak için özenle çalışmalısınız.

- **Net Plan ve Sahiplik** - Kurtarma operasyonları birçok kişinin aynı anda birçok farklı görevi yerine getirmesini içerir, bu nedenle Kesin karar verme ve kriz ekibi arasında iyi bilgi akışı için operasyon için bir proje lideri gerekir.

- **Paydaş iletişimi** - Kurumsal paydaşlar için zamanında güncellemeler ve aktif beklenti yönetimi sağlamak için iletişim ekipleriyle birlikte çalışın.

İPUÇLARI

- **Yeteneklerinizi ve sınırlarınızı bilin** - Büyük güvenlik olaylarını yönetmek çok zor, çok karmaşık ve sektördeki birçok profesyonel için yenidir. Ekipleriniz bunaldıysa veya bir sonraki adımda ne yapacaklarından emin değillerse, dış kuruluşlardan veya profesyonel hizmetlerden yararlanın.

- **Çıkarılan dersleri yakalayın** - Yazılı prosedürler olmadan yaşadığınız ilk olay olsa bile, güvenlik operasyonları için role özel el kitapları oluşturun ve sürekli olarak geliştirin.

İletişim

Canlı bir olay sırasında iletişimi yönetmek, şirketlerin karşılaşabileceği diğer kriz türleriyle karşılaştırıldığında benzersiz zorluklar ortaya çıkarır. Bir şirketin kaybedilen bilginin kapsamı, saldırganların ne kadar süredir sistemde olduğu ve düzeltme adımlarının onları sistemlerden uzak tutmada başarılı olduğunun teyidi hakkında bildikleri, adli tıp incelemesi yapmak için gereken birkaç hafta boyunca büyük ölçüde değişecektir. Sonuç olarak, bir olayla ilgili yanlış bilgi iletme riski vardır ve bu da nihayetinde kurumun itibarının daha fazla zarar görmesine neden olabilir.

KRİTİK BAŞARI FAKTÖRLERİ

Her olayın kendine özgü bir stratejisi olsa da, bu kararları verirken akılda tutulması gereken birkaç temel ilke vardır.

- **Sonuçlara değil eylemlere odaklanın.** Bir olayın erken safhalarında, iletişimde şirketinizin güvenlik olayını araştırmak ve düzeltmek için attığı adımlara odaklanın. Bu genellikle kolluk kuvvetlerine haber verme, soruşturmaya yardımcı olması için adli tıp uzmanlarını işe alma ve sorunu düzeltmek için atılan genel adımlar gibi adımları içerir. Bu gerçeklerle ilgili adli bir kesinlik oluşana kadar rakamları açıklamaktan veya olayın kapsamını başka bir şekilde belirlemekten kaçının.

- **Müşterileri kuzey yıldızınız olarak tutun.** Tüm mesajlarınızda, müşterilerin korunmasına nasıl yardımcı olduğunuza odaklanın. Medya genellikle saldırının kendisi hakkında daha fazla ayrıntı ya da olayın aydınlatılmasına yardımcı olacak diğer gerçekleri öğrenmek isteyecektir. Ama daha ilginç ya da sansasyonel bir hikaye/haber yayınlamak isteyecektir. Ancak, bu ayrıntılar genellikle müşterilerin endişelerini veya ihtiyaçlarını gidermeye yardımcı olmaz. Uygulanabilir rehberlik sağlamaya odaklanmak, muhtemelen müşterileriniz için daha yararlı olacaktır.

- **Medya etkileşimlerini işlemsel tutun.** Bir güvenlik olayı sırasında amaç, olayın haberlerde yer almasını engellemek ve şirketin temel mesajlarının haberlerde yer aldığını teyit etmektir. Bu hedeflere ulaşmanın en etkili yolu medyaya yazılı açıklamalar sunmak ve yalnızca gerektiğinde bir sözcüyle röportaj yapılmasına izin vermektir.

- **Sahip olduğunuz mülklerden yararlanın.** Bir olayla ilgilenenlerin doğru ve güncel bilgilere ulaşabileceği tek bir çevrimiçi hedef oluşturmak iletişimin kolaylaştırılmasına yardımcı olabilir. Bu sitede yayınlanan bilgiler, şirket yönetiminden gelen bir müşteri mesajını, müşterilerin sormasını beklediğimiz Soru-Cevapları ve müşterilere yardımcı olabilecek diğer kaynaklara bağlantıları içerebilir.

DİĞER İLETİŞİM EYLEMLERİ

İletişimi etkili bir şekilde yönetmek, doğru dış mesajları paylaşmanın çok ötesine geçer. Etkili bir müdahale sürecinin parçası olarak başka bazı eylemler de dikkate alınmalıdır.

- **Dahili kitleleri bilgilendirin.** Müşteriye dönük çalışanların olay hakkında bilgilendirildiğini ve soruları olması halinde uygun konuşma noktalarının veya eskalasyon süreçlerinin sağlandığını teyit edin.

- **Sohbeti izleyin.** Bir soruşturmanın erken aşamalarında medya sızıntılarını tespit etmek ve ardından bir sorun açıklandıktan sonra duyguları anlamak için krize özel geleneksel ve sosyal medya izleme geliştirin. Konuşmaların iyi bir muhasebesi olmadan, bir olay ortaya çıkarken karar vermek zordur.

- **Güveni yeniden kazanmak veya kazandırmak için atılacak adımları değerlendirin.** Her zaman gerekli olmasa da, şirketinizin bir olay sonuçlandıktan sonra müşteri güvenini yeniden kazanmak için atması gereken adımlar olup olmadığını değerlendirmesi önemlidir.

Yasal

Bir siber güvenlik olayı, mevzuata uygunluk, yasal ve sözleşmesel bildirim yükümlülükleri ve takip eden dava ve düzenleyici yaptırım işlemleri ve soruşturmaları riskinin yönetilmesi açısından çeşitli zorluklar ortaya çıkarır. Sonuç olarak, hukuk müşavirleri olaylara müdahalenin yanı sıra proaktif siber güvenlik programı geliştirme, uygulama ve yürütmede giderek daha kritik bir rol oynamaktadır.

Bir soruşturmayı yönetmek üzere hukuk müşavirinin erkenden görevlendirilmesi, bu yükümlülüklerin belirlenmesine ve düzenleyiciler, davacılar, hissedarlar ve sektör gruplarından kaynaklanan yasal risklerin yönetilmesine önemli ölçüde yardımcı olabilir.

Yasal riskleri yönetirken yasal yükümlülüklere uyum için akılda tutulması gereken birkaç temel ilke vardır:

- **Gizliliği Koruyun ve Ayrıcalıkları Koruyun.** Hukuk müşaviri (dahili ve/veya harici), yasal yükümlülükleri belirlemek ve riski yönetmek için genellikle BT güvenlik lideriyle yakın işbirliği içinde soruşturma ve müdahale çabalarını yönlendirecek şekilde konumlandırılmalıdır. Hukuk müşaviri soruşturmayı yönetirken, iletişimler ve çalışma ürünleri yasal ayrıcalık kapsamına girer ve bu da önemli bir gizlilik koruması sağlar.

- **Yasal, Sözleşmesel ve Diğer Yükümlülükleri Belirleyin.** Yasal bildirim yükümlülükleri değiştirildikçe ve (yeniden) yorumlandıkça, bildirim yükümlülüklerini tetikleyen veri unsurları ve olaylar değiştikçe ve sözde bildirim güvenli limanları yaratıldıkça yasal yükümlülükler sürekli değişmektedir. Ayrıca, sözleşme ve sektör kuralları genellikle yasal yükümlülüklerden daha geniştir ve güvenli limanlara tabi değildir. Bildirim yapma kararı - ve neyin iletileceği - adli soruşturmaların genellikle sonuçsuz olduğu ve kanıt kayıtlarının kusurlu olduğu gerçeği ile daha da zorlaşmaktadır. Bu kararları, değişen yasal yorumların yanı sıra kabul edilen ve beklenen uygulamalar ışığında dikkatle değerlendirin.

- **İhlal Sonrası Eylemler/ Beyanlar Konusunda Dikkatli Olun.** Ne söyleneceğini ve ne söylenmeyeceğini anlamak, yasal riski yönetmek için kritik öneme sahiptir. Davacılar düzenli olarak olay sonrası eylemleri ve iletişimleri kullanarak olayın niteliği, etkilenen bireylerin kapsamı ve davalarını mahkemede canlı tutacak zararlar hakkında argümanlarda bulunurlar. İletişim ve mesajlaşmaya ek olarak önemli ve esaslı iletişim ekibinden gelen girdiler, etkilenen bireylere yönelik tüm iletişimler ve ihlal sonrası düzenlemeler hukuk tarafından dikkatle incelenmelidir.

- **Kolluk Kuvvetlerinin Katılımını Sağlayın.** Kolluk kuvvetlerini devreye sokmak artık olay müdahalesinde önemli bir husustur. Bu yalnızca iletişim anlatısının önemli bir parçası olmakla kalmaz, aynı zamanda sektöre (örneğin, belirli devlet yüklenicileri) ve etkilenen veri türüne (örneğin, bir kredi kartı ihlali durumunda bankalar tarafından) bağlı olarak genellikle gereklidir. Uygun şekilde kolaylaştırılmış kolluk kuvveti katılımı da bazen yasal bildirimleri geciktirmek, olayla ilgili ek bilgi edinmek ve temel nedenleri ve/veya tehlikeye atılan verileri belirlemeye yardımcı olmak için kullanılabilir. Hukuk departmanı, en azından kolluk kuvvetlerinin soruşturma için bilgi

edinmek amacıyla kullandığı yasal süreci müzakere etmek ve yönetmek için bu tür bir erişimi koordine etmelidir.

- **Yöneticileri/Yönetim Kurulu Üyelerini Yeterince Bilgilendirin.** Hissedarlar ve düzenleyiciler, C-suite ve yönetim kurulu üyelerinin siber güvenlik olaylarına katılımını ve bu olayların gözetimini giderek daha fazla incelemektedir. Yöneticilere ve yönetim kurulu üyelerine yönelik güncellemeler, güvene dayalı sorumluluklarını yerine getirmelerini ve iş muhakemelerini kullanmalarını sağlayacak bilgilerin niteliği ve niceliği arasında denge kurmalı ve teknik ayrıntılarla aşırı yüklenmelerini önlemelidir.

Referans Listesi

1. Ulusal Standartlar ve Teknoloji Enstitüsü Kritik Altyapı Siber Güvenliğini Geliştirme Çerçevesi, Sürüm 1.1 Ocak, 2017 https://www.nist.gov/cyberframework

2. Ulusal Standartlar ve Teknoloji Enstitüsü, https://www.nist.gov

3. Standartlar ve Teknoloji Enstitüsü Siber Güvenlik Olay Kurtarma Kılavuzu https://doi.org/10.6028/NIST.SP.800-184

4. Microsoft Ayrıcalıklı Erişimin Güvenliğini Sağlama Yol Haritası, http://aka.ms/sparoadmap

5. Güvenlik İstihbarat Raporu, www.microsoft.com/sir

6. EY Küresel Bilgi Güvenliği Araştırması 2016-2017, https://www.ey.com

7. Edelman Gizlilik Risk Endeksi, http://www.edelman.com/insights

"Eğer ataçlarınızı ve elmaslarınızı eşit güçle korursanız, kısa süre içinde daha fazla ataç ve daha az elmasa sahip olursunuz."