SİBER GÜVENLİK KONTROL LİSTESİ

Emre ERKIRAN

Bilgi Güvenliği Uzmanı
ISO 27001 Lead Auditor

Güvenilir bir siber güvenliğin uygulanmasındaki temel zorluklardan biri, uğraşmanız gereken çok fazla şey olmasıdır. Firmalar, kendi finansal kaynaklarını, personelini, uyumluluk gereksinimlerini ve kendi risklerini tüm hassas tehditlerini potansiyel tehditlerden korumak için yeterli olacak bir korumayı şekillendirmeye çalışırken bir yandan işlerin devamlılığına, sürekliliğine odaklanırlar.

Tüm bunları yapabilmek için kilit unsurlardan biri, uygun bir birleşik bilgi güvenliği stratejisini formüle etme kabiliyetidir. Tamamlanması gereken açık ve mantıklı bir kontrol listesi içeren bir stratejidir. Bu tür siber güvenlik kontrol listelerinin birçok örneği mevcuttur, kendi bakış açıma göre ise bunlar çok genel ve çok kullanışlı oldukları için formüle edilmiştir. Her şirketin, kendileri için yararlı olacak kendi siber güvenlik kontrol listelerini oluşturmak için mevcut uyumluluk gerekliliklerini ve en iyi bilgi güvenlik uygulamalarını kullanması, daha iyi yol almada var ise "road map" planında iyi bir seçenektir. Siber güvenlik planlama kılavuzunda, kendi siber güvenlik kontrol listenizin nasıl yapılacağına dair bazı önerilerim olacak.

İlk bölümde kendi kontrol listenizi oluşturmanın arkasındaki genel ilkelerden; ikinci bölümde, şirketinizi hem içeriden hem de dışarıdan gelen tehditlerden nasıl koruyabileceğinizle ilgili daha ayrıntılı bilgilerden bahsedeceğim.

Siber güvenlik kontrol listelerinin üç ilkesi:

Siber güvenliği uygularken, ne yapacağınızı bilmek yeterli değildir, ayrıca nasıl yapılacağını da anlamanız gerekir. Hangi ölçütü kullanacağınızı, aşağıya koyduğunuz önlemlerden en yüksek değeri alabilmek gerekir.

Birçok BT güvenlik yönergesi arasında, etkili önlemleri seçmenize ve bunları etkili bir şekilde uygulayabilmenize olanak tanıyan üç ana ilkeyi formüle edebilirim.

Tutarlılık: Etkili olmayı istiyorsanız, her bir siber güvenlik önlemi tutarlı bir şekilde yönetim kurulunda uygulanmalıdır. Örneğin, iki faktörlü kimlik doğrulaması kullanıyorsanız, yöneticiler ve üst yönetim de dâhil olmak üzere herkesin bunu kullandığından emin olun. Güvenlik politikalarını uygularken yapabileceğiniz en kötü şey, ayrıcalıklı kullanıcılar için istisnalar yapmaya başlamaktır. Bu, yalnızca bu tedbiri uygulamak için çok daha zor olmakla kalmaz, aynı zamanda belirli durumlarda ölçütün olumlu etkilerini tamamen geçersiz kılabilir.

Holizm: Siber güvenlik bir bütün olarak ele alınmalıdır. Verileriniz içeriden gelen tehditlerden yeterince korunmadığında, çok sağlam ve sıkı bir şekilde korunan bir çevre oluşturmanın hiçbir anlamı yoktur. Dengeli, katmanlı bir savunma uyguladığınızdan ve verilerinizi karşılaştığı herhangi bir tehditten korumanıza ve herhangi birini küçümsememenize imkân verecek şekilde gerçekleştirdiğinizden emin olun.

Riske dayalı yaklaşım: Güvenlik stratejisini oluştururken ve uygularken, dikkate alınması gereken en önemli şey şirketin karşı karşıya olduğu mevcut risklerdir. Riske dayalı bir yaklaşım benimsemek ve verilerinizin karşılaştığı mevcut güvenlik açıklarını ve tehditlerini belirlemek için kapsamlı bir risk değerlendirmesi yapmak ve bunları karşılamanın en iyi yoluna karar vermek gerekir. Uyumluluk gereksinimlerinin her zaman değiştiği gerçeğinin dışında, aldığınız önlemlerin şirketinizin güvenlik ihtiyaçları ile tutarlı olduğundan emin olmanız gerekir.

Yukarıda bahsi geçen bu üç ilkeyi takip ederek, sadece uygun bir kontrol listesi oluşturmuş olmazsınız, aynı zamanda planlanan tüm önlemleri mümkün olan en etkili şekilde uygulayabilirsiniz.

Siber güvenlik kontrol listenizi formüle etme: Başarılı siber güvenlik politikasını uygularken göz önünde bulundurulması gereken pek çok şey vardır. Şirketinizin gerekli tüm önlemleri aldığından emin olmak için kendi kontrol listenizde yer almasını isteyebileceğiniz ilgili adımların bir listesini paylaşacağım.

- Fiziksel olarak güvenli veriler: Muhtemelen hassas bilgilerinizi korumak için en temel önlem bu bilgilere fiziksel erişimin kısıtlandığından emin olmaktır. Sunucularınızın yalnızca ofisinizin ziyaretçilerine (veya bu konuda rastgele insanlara) değil, aynı zamanda kendi çalışanlarınıza da yeterince açık olmadığından emin olun. IaaS'yi kullanıyorsanız ya da sadece bir veri merkezinden altyapı kiralıyorsanız, bu gerçekten sizin endişelenmeniz gereken bir durum değildir. Ancak kendi fiziksel sunucularınıza sahipseniz ve bunları barındırıyorsanız, bunların yeterince korunmasını sağlamalısınız.

- Fiziksel olarak güvenli ağ erişim noktaları: İç kurumsal ağınızın erişim noktalarının güvenli olduğundan emin olmalısınız. Bu sadece çalışan cihazlar gibi belirgin şeyleri değil, şirket Wi-Fi ve Ethernet çıkışı gibi konuları da içerir. Konukların şirketinizin Wi-Fi'ını kullanmasına izin veriyorsanız, iç ağınıza erişemediğinden emin olun ve yönlendiricinizin ve diğer cihazların varsayılan olmayan benzersiz parolalara sahip olduğundan emin olun. Herhangi bir erişim noktası savunmasızdır ve dolayısıyla güvenliğin ciddiye alınması gerekir.

- Çalışan arka plan kontrolleri yapın: Kendi çalışanlarınız şirket verilerinizin güvenliği için en büyük tehdidi oluşturabilir. Potansiyel iç tehditleri dikkate almak ve bunlarla mücadele etmek için önlemler almak gereklidir. Yapabileceğiniz ilk ve en belirgin şey ayrıntılı arka plan kontrolleridir. Çalışanlarınızdaki arka plan bilgilerinin kontrol edilmesi çok fazla çaba gerektirmez. Bu, adlarını aramak ve size verdikleri bilgileri doğrulamak için önceki çalışma yerlerini aramak kadar basit bir şey olabilir. Böyle basit bir arka plan kontrolü, içerideki tehditlerden % 100 korunma sağlamayacaktır, ancak en belirgin suçluları filtrelemenize izin verecektir. Mesela en son çalıştığı yerde herhangi bir disiplin cezası almış mı, güvenlik ihlali gerçekleştirmiş mi gibi...

- Çalışan farkındalığı: Çalışanlarınızın, şirketinizin karşı karşıya kaldığı veri güvenliği tehditlerine ve başarılı bir saldırının ortaya çıkarabileceği tehlikeye karşı tamamen haberdar olduklarından emin olun. Çalışanları, kimlik avı, sosyal mühendislik ve onları hedefleyebilecek diğer tekniklerin tehlikeleri konusunda eğitin ve bu tür tehditlere yeterince yanıt vermelerini öğretin.

- Güvenlik duvarını yapılandırın ve sürdürün: Güvenlik duvarı, ağınızı korumanın en temel yollarından biridir ve kesinlikle her şirket tarafından kullanılmalıdır. Ancak, güvenlik duvarınızı doğru bir şekilde yapılandırmak ve işinizi etkili bir şekilde yaptığınızdan emin olmak da önemlidir. Örneğin, hem gelen hem de giden trafiği sınırlandırmanız, gerekli uyarıları yapılandırmanız ve soruşturma sırasında kullanılabilecek günlüğü ve geçmişi etkinleştirmeniz gerekir.

- Anti-virüs yapılandırın: Her şirketin yapması gereken bir diğer temel siber güvenlik önlemi, bir virüsten koruma yazılımını kurmak ve uygun şekilde yapılandırmaktır. İdeal durumda, kötü amaçlı yazılımlardan ve bilgisayar korsanlığından korunmanızı güçlendirebilir, ancak bazen yanlış sonuçlar üretebilir veya tehlikeli yazılımları tamamen atlayabilir. Bu nedenle, bunu önlemek ve virüsten korunma etkililiğinizi en üst düzeye çıkarmak için, gerekli tüm özel durumları yapılandırdığınızdan ve her zaman güncel tuttuğunuzdan emin olun.

- Trafiği filtrelemek için web filtreleri oluşturun: Verilerinizi koruyabilmenin ve şirketinizin sıkıntılarını ortadan kaldırmanın bir başka yolu da, güvenlik duvarının kendisinde, özel yazılım veya sistem ayarları gibi başka yollarla web trafiğini filtrelemek.

- Bileşen korumasını koruyun: Bileşenlerin her birinin bütünlüğünü korumaktır. Bu, tüm yönlendiricileriniz gibi şirket ağınızı oluşturan her aygıtın fiziksel olarak erişilememesi gerektiği, ancak aynı zamanda karmaşık olmayan benzersiz bir varsayılan parola ile korunacağı anlamına gelir.

- İletişimi şifreleyin: Ağınızdaki tüm iletişimler şifrelenmelidir. Ayrıca gelen ve devam eden tüm trafiği olabildiğince şifrelemek iyi bir fikirdir. Bu tür şifrelemeler,

verilerin orta saldırıdaki bir adam tarafından yakalanmasını veya ağınızda zaten bulunan bir fail tarafından çalınmasını engelleyecektir.

- Trafiği izleyin: Yerleşik sistem özellikleri ve özel trafik izleme çözümleri dâhil olmak üzere trafiğinizde sekmeleri güvenli tutmanın birçok yolu vardır. Trafik izleme; şüpheli ağ etkinliğini gibi hassas verilerinizi dışarıya ileten kötü amaçlı yazılımları tespit etmenizi sağlar. Ayrıca bir soruşturma durumunda çok değerli olabilir.

- Önemli sistemler için yedek bağlantıları koruyun: Güvenliğiniz kadar sisteminizin genel güvenilirliği ile ilgili bir başka hayati önlem, kritik sistemler için yedekli bağlantıların olduğundan emin olmaktır. Bu, ağınızın güvenliğinin ihlal edilmesi durumunda çalışmaya devam etmenizi sağlar ve hizmet reddi saldırıları (DoS - Denial of Service Saldırısı - Hizmet Reddi Saldırısı) gibi belirli saldırı türlerini atlatmanıza yardımcı olabilir.

- Düzenli yedekleme uygulaması oluşturun: Yedeklemeler, sistemi yalnızca uğraşması zor olan (ransomware gibi) belirli saldırılardan korumakla kalmaz, aynı zamanda saldırıdan sonra sistemi geri yüklemek için bir yol görevi görür. Yedeklemelerin her zaman güncel olduğundan emin olmanız çok önemlidir.

- Yedeklemeleri güvenli bir şekilde saklayın: Yedeklemeler güvenli bir şekilde yapılmalı ve saklanmalıdır. Bir yedekleme işlemi üzerinde işbirliği yapmak için birkaç farklı kişi atamak en iyisidir. Bu, kötü niyetli içeriğe sahip kişilerden kaynaklanan riskleri büyük ölçüde azaltır (insanlar diğerleriyle işbirliği yaparken kötü niyetli eylemleri gerçekleştirme veya erişimi kötüye kullanma olasılığının düşük olması gibi) ve yedekleme işleminin doğru şekilde yapılmasını sağlar. Ayrıca, yedeklerinizi şifrelemek ve bunları ana ağınızdan ayrı olarak erişilemeyen bir yerde saklamak, böylece bir ihlal durumunda ele geçirilmeyeceklerini garanti etmeniz gerekmektedir.

- Tüm tehdidi ciddiye almak: Yukarıdaki adımların tamamı ve en iyi uygulamaların listesi, temel olarak bilgi güvenliği denetimi kontrol listesi tasarlarken mükemmel bir şablon görevi görebilir. Bu adımların çoğu güvenli bir çevre oluşturmayı ve verilerinizi kötü amaçlı yazılımlardan, hizmet reddi saldırılarından, fidye yazılımlarından ve diğer harici ihlallerden korumayı amaçlamaktadır. Ancak bu şirketinizin karşı karşıya olduğu tek tehdit değildir. Organizasyon içerisinden saldırı, herhangi bir hack veya ihlalden çok daha zararlı ve maliyetli olabilir. Tüm şirketler içeriden koruma tehdidi almazlar - ve sonuç olarak, birçoğu uygun korumayı yerine getiremeyerek kendi savunmasını zayıflatır. Dolayısıyla siber tehdit ve risklere karşı daima tedbirli olunmalıdır. Siber güvenlik kontrol listesini bu minvalde oluşturacağınız güvenli günler diliyorum…