Etkin siber güvenlik stratejisi oluşturma

Küçük ve Orta Ölçekli İşletmeler için Kılavuz

ESET
Digital Security
Progress. Protected.

Büyük şirketlerde, şirketin siber güvenliğini denetleyen ve etkin stratejiler oluşturan departmanlar genellikle vardır. Ancak, personel kadrosu içinde sadece birkaç BT uzmanı olan küçük ve orta ölçekli işletmeler (KOBİ'ler) ne yapacak? Olası tüm önlemleri almakla uğraşan bu kuruluşlar, uygun şekilde korunduklarından nasıl emin olacak?

Size **ESET KOBİ ve MSP Bölüm Başkan Yardımcısı Michal Jankech**'ten birkaç ipucunu aktaralım.

ESET
Digital Security
Progress. Protected.

Nereden başlamak gerekir?

KOBİ'lerin birçoğunda, çalışanlar arasında dijital güvenlik stratejisinden sorumlu az sayıda personel vardır. Bu nedenle, en büyük tehditlere odaklanmaları ve tüm enerjilerini şirket faaliyetlerinin aksamaması için bu tehditlere ayırmaları çok önemlidir.

KOBİ'lerin öncelikle aşağıdaki alanları ele alması gerektiğini ekleyen Jankech, "**En önemli güvenlik açıklarını belirlemeyi içeren risk tabanlı bir yaklaşım benimsemeliler**" diye açıklıyor.

- **Veri koruma ve şifreleme**
- **Çok katmanlı uç nokta koruması ve kullanıcı erişim kısıtlamaları**
- **MFA ve düzenli güncellemeler**
- **Nitelikli e-posta sağlayıcılar ve çalışan eğitimi**
- **İyi ve eksiği olmayanlar için EDR ya da MDR**

Veri koruma ve şifreleme

Tüm cihazlarınız bir kullanıcı adı ve güçlü bir parola ile güvencede mi? Harika. Ancak yine de, cihazlarınızı olabildiğince güvenli hale getirmek istiyorsanız yapmanız gereken başka şeyler var. "**Tüm uç noktaların şifrelenmesi gerekir**. Bilgisayarınızın çalındığını düşünün. Şifre ve kullanıcı adını bilmedikleri için içeri giremeyecekler ama yine de sabit diski çıkararak verilere ulaşabilirler. Jankech, yalnızca taşınabilir cihazların değil, masaüstü bilgisayarların da düzgün bir şekilde şifrelendiğinden emin olun" diyor.

"Bir keresinde bir sağlık kuruluşuna gittim ve kioskun hemen yanına konulan bilgisayarın şifre ile korunmadığını gördüm. Birisi kolaylıkla içeri girip bilgisayarı çalabilir ve tüm hasta verilerine erişim sağlayabilirdi. Bu tür senaryolar etkin veri koruma ve şifreleme önlemleri uygulanarak önlenebilir."

Çok katmanlı uç nokta koruması ve kullanıcı erişim kısıtlamaları

“Yönetici kullanıcı hesaplarını sınırlamak çok önemlidir. Birçok durumda, en büyük zarara yol açan kişilerdir. Jankech, bir sabotajcı, yönetici hesabına erişirse cihaza potansiyel olarak her şeyi yükleyebilir,” diyor.

Ayrıca, tek koruma katmanının yeterli olmadığını da unutmayın. “Bu bir aile evini korumaya benziyor. Böyle bir durumda, giriş kapısı, güvenlik kapıları, alarm, çit ve pencereler kullanarak savunmanızı güçlendiren önlemler alırsınız. ... Birçok insan **antivirüs çağının sona erdiğini** söylüyor. Evet, yalnızca imzalarla çalışan standart antivirüs çağı sona erdi. Jankech, bu tür çözümler, çok çeşitli mevcut tehditleri kapsayamaz,” diye devam ediyor.

Bunun yerine, makine öğrenimi ilkelerine dayalı ve davranış tipi koruma sunan, tehlikeli web sitelerini kara listeye alan ve ağ saldırılarına ya da uzak masaüstü protokolündeki kötüye kullanılabilecek güvenlik açıklarına karşı koruma da dahil olmak üzere, riskli etki alanlarına erişimi engelleyen, **çok katmanlı uç nokta güvenlik yazılımı** öneriliyor.

> **KOBİ’ler için en çok önlem almaya yatırım yapmak anlamlıdır. Sistemlerinizi güçlendirmek, güncel kalmalarını sağlamak ve iyi bir uç nokta koruma yazılımı kullanmak çok önemlidir.**
>
> **Michal Jankech**,
> ESET KOBİ ve MSP Bölüm Başkan Yardımcısı

Jankech, “Yalnızca bir koruma yazılımına sahip olmakla işiniz bitmiyor, aynı zamanda doğru şekilde yapılandırmak ve güncelleme de çok önemlidir” diye ekliyor. Örneğin, uç nokta koruma yazılımının kaldırılamayacağından veya yapılandırmasının değiştirilemeyeceğinden emin olmak zorundasınız.

Daha sonra, **uç noktalar için bir yönetim paneli kullanın**. “Birçok şirket, uç nokta koruma istemcisi kullanmanın yeterli olduğunu sanıyor. Ama tüm ağı denetlemenizi sağlayan bir panel aracılığıyla yönetmezseniz, düzgün çalışıp çalışmadığını asla bilemezsiniz. Jankech, şirkette yalnızca 10 bilgisayarınız olsa bile, özellikle insanların her geçen gün daha fazla evden çalışıp seyahat ettiği günümüzde, bunları düzgün bir şekilde kontrol edemezsiniz” diyor. Aynı zamanda, panel size sistemlerinizin ve ağ trafiğinizin ideal durumda olduğundan %100 emin olmanız için kontrol raporları vermelidir.

MFA ve düzenli güncellemeler

Tüm iş cihazları ve kişisel cihazlarda, çok faktörlü kimlik doğrulaması (MFA) bulunmalıdır. Ayrıca, tüm işletim sistemlerinin en son sürümlerinin kullanılmasını sağlayın. Jankech, "İhlallerin çoğu kimlik ve parola hırsızlığı ya da işletim sisteminde kötüye kullanılabilen, yaygın olarak bilinen bir güvenlik açığı nedeniyle ortaya çıkıyor" açıklamasını yapıyor.

İşletim sisteminin her yeni sürümünde, satıcı olası açıkları düzeltir ve siz de, siber suçluların şirket cihazlarına sızma ihtimalini azaltmış olursunuz. **Otomatik güncelleme önerilir.** "KOBİ'lerde, sıfırıncı gün saldırıları nadiren görülür.

Amaca yönelik yazılımlar kullanıyorsanız siber suçluların bu tür hedefe yönelik bir saldırı gerçekleştirme olasılığı oldukça düşüktür. Jankech, birçok durumda, yaygın olarak kullanılan ya da açık kaynaklı yazılımlarda sıkça karşılaşılan güvenlik açıkları, kuruluşunuza sızma noktalarıdır" diyor.

> **"Doktorlar, mimarlar, halkla ilişkiler şirketleri... hepsinin birer siber güvenlik stratejisine ihtiyacı var.
> Örneğin, bir çok kişi belirli belgelerin telif hakkıyla korunduğunun ve dolayısıyla da, buna uygun olarak kullanılması gerektiğinin farkında değildir."**
>
> **Michal Jankech**,
> ESET KOBİ ve MSP Bölüm Başkan Yardımcısı

Nitelikli e-posta sağlayıcılar ve çalışan eğitimi

Güvenilir e-posta sağlayıcılar da önemlidir. "Ayrıca, çalışanlar bir kimlik avı e-postasını nasıl tespit edeceklerini de bilmelidir. Jankech, ayrıca her alıcının mesajın şirket dışından geldiğini bilmesini de sağlayabilirsiniz - Office 365 bile e-postaları "harici" etiketiyle işaretlemenize izin veriyor", tavsiyesinde bulunuyor. Farkındalığı artırmak için zaman zaman, siber güvenlik çalışanlarının eğitimine yatırım yapmak yararlıdır. ESET Dijital Güvenlik Kılavuzu'nda eğitimi nasıl etkin ve keyifli hale getirebileceğinizle ilgili **birkaç ipucuna göz atabilirsiniz**.

Jankech, çoğu şirketin bu temel önlemleri uygulamadığını ve bazen büyük işletmelerin dijital güvenliğinde daha da önemli boşluklar olduğunu vurguluyor. "Bazı şirketler hâlâ siber güvenlik çözümlerine yatırım yapmak konusunda tereddüt ediyor ya da iş alanlarının pek de çekici olmaması nedeniyle hedef haline gelmeyeceklerini düşünüyor. Ama genelde, siber saldırılar hedefe yönelik değildir. Siber güvenlik uzmanı, herkes kurban olabilir" açıklamasını yapıyor.

İyi ve eksiği olmayanlar için EDR ya da MDR

Tüm temel siber güvenlik yapı taşlarını sağlam bir şekilde yerleştirdikten sonra, **Uç Nokta Algılama ve Yanıt (EDR) çözümleri gibi gelişmiş siber güvenlik araçlarını** değerlendirmenin zamanı gelmiştir. "Bu, tehdit önlemenin her zaman başarısız olacağı varsayımı üzerine inşa edilmiş, tamamen yeni bir alt pazardır. Ürün setinin bu bölümü çoğunlukla, çok sayıda şirket içi BT departmanı ve 7/24 çalışan bir şirket içi SOC [güvenlik operasyon merkezi] maliyetini karşılayabilen büyük kuruluşlar için geçerlidir. Jankech, bu yaklaşımda olmak, genellikle siber suçluların eninde sonunda sisteminize başarılı bir şekilde saldıracağı düşüncesini benimsemek anlamına gelir" diye ekliyor.

EDR çözümleri ağdaki anormallikleri ve şüpheli davranışları tespit eder ve uygun şekilde süreci bloke ederek yanıt vermenizi sağlar ya da sistemler bu görevleri özel otomatik kurallar aracılığıyla yapar. "Genellikle daha büyük şirketlerde kullanılsalar da, küçük işletmeler için de faydalı olabilirler.

KOBİ siber güvenlik stratejisinin temelleri

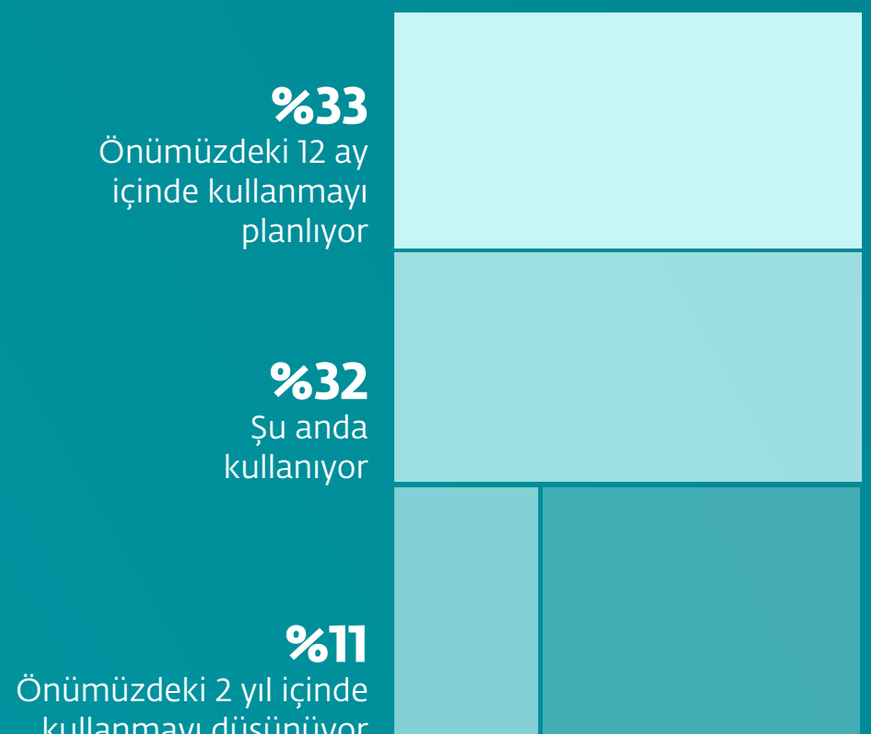
- **Korumalı ve şifrelenmiş veriler**
- **Kullanıcılar için kısıtlı erişim kuralları**
- **Çok katmanlı uç nokta güvenliği**
- **MFA ve işletim sistemi güncellemeleri**

Jankech, her durumda EDR platformunuzu yönetmek için personele ihtiyacınız olacaktır. İmkanı bulunan küçük işletmelerin bu tür hizmetleri dışarıdan almayı düşünmesi önerilir," diye ekliyor.

MDR (Yönetilen Algılama ve Yanıt) burada devreye giriyor. MDR, üçüncü bir tarafça yönetilen EDR'dir. Jankech, "Tek bir izleme merkezinden, onlarca ve hatta yüzlerce müşteri denetleniyor ve genellikle 7/24 ulaşabileceğiniz bir yardım hattı da oluyor" diyor.

Yine de, EDR ya da MDR sadece temelleri kurduysanız düşünülmelidir. Hazır olduğunuzda EDR veya MDR'yi kullanmak, şirketinizin güvende ama her zaman tetikte olması sayesinde, kuruluşunuzun herhangi bir siber saldırıya dayanma şansını artırır.

EDR / XDR / MDR çözümleri kullanımı



Kaynak: 2022 ESET KOBİ Dijital Güvenlik Hassasiyeti Raporu

ESET HAKKINDA

ESET® dünya çapında 30 yılı aşkın bir süredir şirketleri, önemli altyapıyı ve dünya genelindeki tüketicileri gittikçe artan karmaşık dijital tehditlerden korumak üzere işletmeler ve tüketicilere yönelik sektör lideri BT güvenliği yazılımları ve hizmetleri geliştiriyor. Uç nokta ve mobil güvenlikten şifreleme, çok faktörlü kimlik doğrulaması ile uç nokta algılama ve yanıt çözümlerine kadar ESET'in yüksek performanslı, kullanımı kolay ürünleri 7/24 rahatsız etmeden koruyup denetler ve önlemlerini gerçek zamanlı olarak günceller. Böylece kullanıcıları güvende tutarken şirketlerin kesintisiz faaliyet göstermesini sağlar. Gelişen tehditler, teknolojinin güvenli kullanımını sağlayan gelişen bir BT güvenlik şirketi gerektirir. Dünya çapındaki ESET AR-GE merkezleri ortak geleceğimizi desteklemek üzere bu amaca ulaşmak için çalışıyor. Daha fazla bilgi için **www.eset.com.tr** adresini ziyaret edin ya da bizi **LinkedIn**, **Facebook** ve **Twitter**'da takip edin.

Digital Security
Progress. Protected.