TEKNİK İNCELEME

KİLİTLENMEMİŞ KAPILAR

ARAŞTIRMALAR, YAZICILARIN SİBER SALDIRILARA KARŞI KORUNMASIZ KALDIĞINI GÖSTERİYOR

BT ekipleri diğer uç noktalara odaklanıyor, ancak kurumsal yazıcılar güvenlik konusunda geride kalıyor

Yazıcılar çok kolay hedeflerdir: Ağa bağlı çok sayıda yazıcı herhangi bir sınırlamaya sahip değildir ve güvenli bir şekilde kilitlenmemiştir.

Ancak tehdit oldukça ciddidir ve ihmal edilmemelidir. Kurumsal sınıf yazıcılar, ağınızdaki diğer uç noktalarla aynı güvenlik açıklarına sahip olan ağa bağlı, güçlü aygıtlar haline gelmiştir. Genellikle güvenli olmayan bu uç noktalar, siber saldırıların gerçekleşme olasılığını kolaylaştırmanın yanı sıra şirketinizin mali ve gizli bilgilerine erişilmesine neden olarak ciddi ticari sonuçlara yol açabilir.

Buna rağmen, kısa süre önce Spiceworks tarafından 300'ün üzerinde kurumsal BT karar vericiyle gerçekleştirilen bir anket, masaüstü/dizüstü bilgisayar ve mobil aygıtlara göre çok daha düşük oranla görüşülen kişilerin yalnızca %16'sının yazıcıların güvenlik tehdidi/ihlali açısından risk oluşturduğunu düşündüğünü ortaya koymuştur.[1] Böylesi bir algı, BT personelinin ağ güvenliğine yaklaşımını olumsuz etkilemektedir. Her beş kuruluştan yaklaşık üçünde yazıcılar için güvenlik uygulamaları bulunuyor olsa da bu oran, diğer uç noktalar için söz konusu olan güvenlik uygulamalarından çok daha düşüktür ve çok kolay çözümlerle korunabilecek yazıcıların savunmasız kalmasına yol açmaktadır.

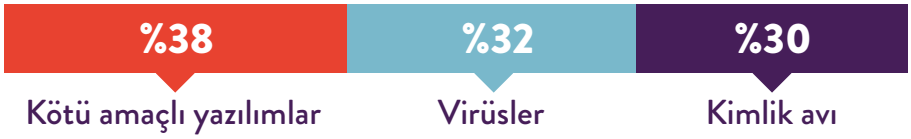
Bu teknik incelemede, Spiceworks tarafından gerçekleştirilen anketin sonuçlarına göre yazıcı güvenliğine yönelik veriler, güvenlik ihlallerinin etkileri ve siber saldırılara karşı koruma sağlayan modern dahili yazıcı güvenlik özellikleri sunulmaktadır.

GÖRÜŞÜLEN KİŞİLERİN **YALNIZCA %16'SI** YAZICILARIN YÜKSEK GÜVENLİK TEHDİDİ/İHLALİ RİSKİ ALTINDA OLDUĞUNU DÜŞÜNÜYOR.[1]

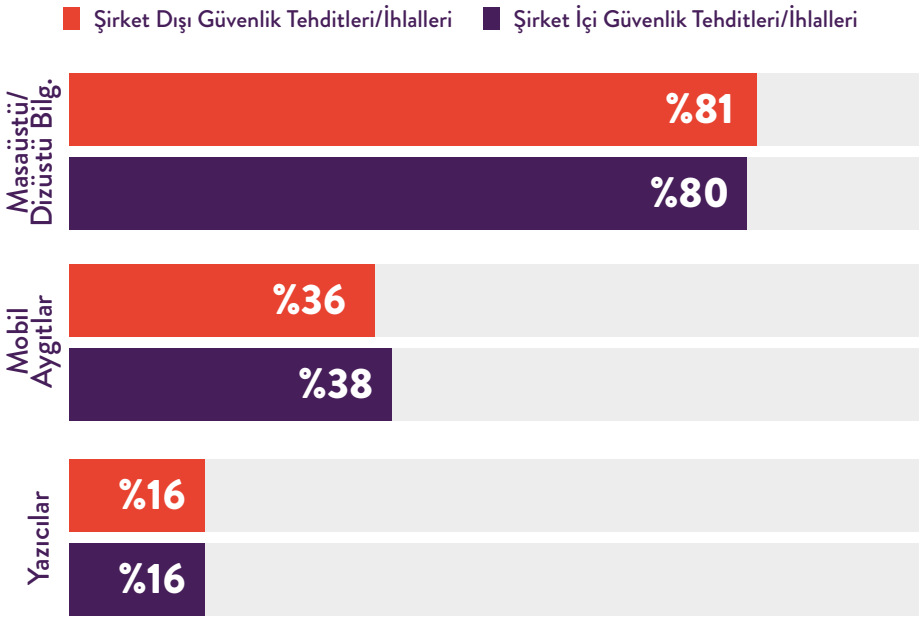
SALDIRILARA AÇIK KAPILAR

Spiceworks anketinde görüşülen kişilerin %74'ü (net), kuruluşlarında geçen yıl içinde herhangi bir harici BT güvenlik tehdidi veya ihlali yaşadıklarını belirtmiştir. Görüşülen kişilerin %70'i (net), genellikle kullanıcı hatalarından, kişisel aygıtların iş amacıyla kullanılmasından veya çalışanların bir ev ya da genel ağı iş amacıyla kullanmasından kaynaklanan dahili bir BT güvenlik tehdidi veya ihlaliyle karşı karşıya kalmıştır.[1]

EN SIK KARŞILAŞILAN BT GÜVENLİK TEHDİTLERİ/İHLALLERİ



En büyük tehditler öncelikle masaüstü ve dizüstü bilgisayarlardan sızarken mobil aygıtlar ve yazıcılar da başka tehditlere maruz kalmıştır.[1] (Yazıcılar üzerinden sızan %16 tehdit oranı, 2014 yılında gerçekleştirilen benzer Spiceworks çalışmasında ortaya konan %4 oranından çok daha yüksektir.) Yazıcıların bilgisayarlar ve mobil aygıtlar kadar yakından izlenmediği göz önüne alınırsa, yazıcılar üzerinden gelen tehdit sayısının azımsandığını söylemek de mümkündür.



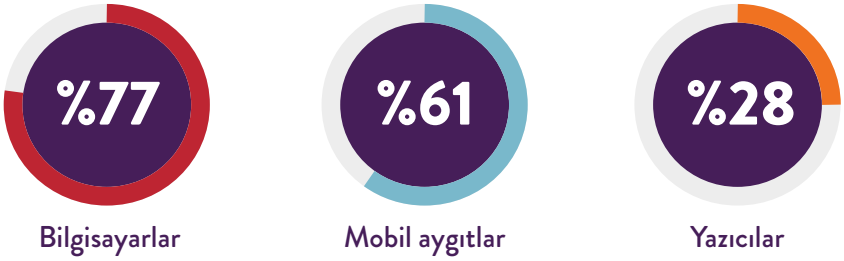
YAZICILARIMIZI İHMAL EDİYORUZ

Her koşulda, Spiceworks tarafından gerçekleştirilen anket yazıcı güvenliğinin sonradan akla geldiğini ortaya koyuyor.

Kuruluşlar ağın, uç noktaların ve veri güvenliğinin öneminin oldukça farkında. Aslında görüşülen kişilerin dörtte üçünden fazlası ağ güvenliği, erişim denetimi/yönetimi, veri koruması veya uç nokta güvenliği çözümleri veya bunların bir birleşimini uyguluyor.[1]

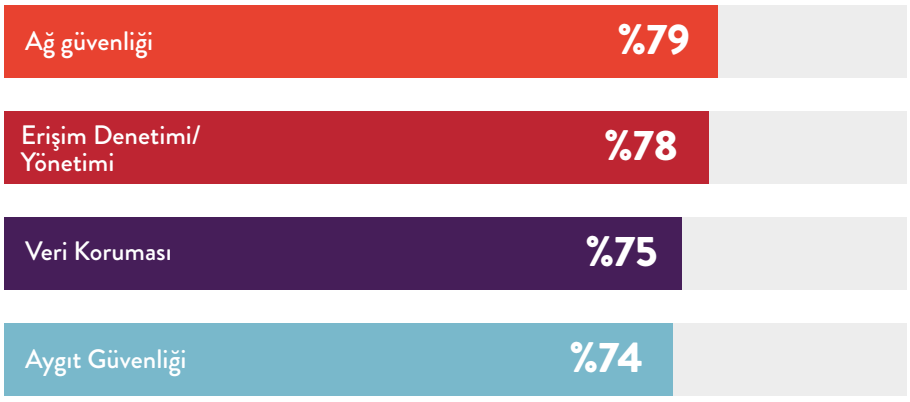
Ancak bu çözümler, yazıcılarda çok daha az kullanılıyor. Görüşülen kişilerin %83'ü masaüstü/dizüstü bilgisayarlarda ve %55'i mobil aygıtlarda ağ güvenliği kullanırken, yalnızca %41'i yazıcılarda ağ güvenliği kullanıyor.[1]

Uç noktaların güvenliği söz konusu olduğunda ise, aradaki fark daha da açılıyor:



Bunun yanı sıra, görüşülen kişilerin %79'u bilgisayarlar ve %54'ü mobil aygıtlar için güvenlik sertifikaları uygulamasına rağmen ankete katılanların üçte birinden daha azı (%28) yazıcılar için güvenlik sertifikaları kullanıyor.[1]

EN SIK KULLANILAN GÜVENLİK UYGULAMALARI



Genel uç nokta aygıtları için kullanılan koruma çözümleri arasından yazıcılar için en sık kullanılan güvenlik önlemleri belge güvenliği, ağ güvenliği ve erişim denetimi çözümleridir. Ancak görüşülen kişilerin yarısından azı kuruluşlarında bu çözümlerden hiçbirinin kullanılmadığını belirtmiştir.[1]

Bazı şirketlerde yazıcılara özel güvenlik uygulamaları bulunsa da bu uygulamalar, yukarıda belirtilenlerden tamamen farklıdır. Kuruluşların %40'tan biraz fazlasında kullanıcı kimliği doğrulaması kullanılırken, %40'tan daha azında web yapılandırma arabirimi için yönetici parolaları kullanılmaktadır.[1] Güçlü bir savunma için her kuruluşun tüm bu yaklaşımların bir karışımını ve daha fazlasını kullanması gerekir.

YAZICILARA ÖZEL EN SIK KULLANILAN GÜVENLİK UYGULAMALARI

Uç nokta uyumu ve denetim uygulamaları söz konusu olduğunda ise, yazıcı güvenlik denetimleri tüm diğer uç noktaların gerisinde kalmaktadır. Kuruluşların yaklaşık %90'ında bir bilgi güvenliği politikası benimsenmiş olsa da yazıcılar genellikle bu politikaların kapsamı dışında kalmaktadır. Örneğin, görüşülen kişilerin %57'si bilgisayarlarında kötü amaçlı yazılımlara karşı koruma bulunduğunu belirtirken, yalnızca %17'si yazıcılarında böyle bir koruma olduğunu belirtmiştir.[1]

HER 10 BT UZMANINDAN YAKLAŞIK 9'U AŞAĞIDAKİ NEDENLERDEN DOLAYI KURULUŞLARINDA BİR GÜVENLİK POLİTİKASI UYGULANDIĞINI BELİRTİYOR:

Açıkça görülüyor ki, kuruluşlar büyük önem verilmesi gereken yazıcı güvenliği konusunu yeterince ciddiye almıyor.

Haziran ayında Computerworld'e konuşan HP baş güvenlik danışmanı Michael Howard, "Çok sayıda yazıcıda halen varsayılan parolalar kullanılıyor ya da hiç parola kullanılmıyor veya on tane yazıcı için aynı parola kullanılıyor" şeklinde konuştu ve şöyle devam etti: "Parola koruması olmayan bir yazıcı, bir korsan için bir hazine demektir. Sık sık karşı karşıya kaldığımız ihlallerden biri, bir yazıcıyı ele geçiren korsanların [gelen belgeleri] baskıdan önce bir dizüstü bilgisayara yönlendirmesi şeklinde gerçekleşen aradaki adam saldırısıdır. Bu saldırılarda, korsanlar CEO'nun baskıya gönderdiği tüm belgeleri görebilir."[2]

YAZICILARA İZİNSİZ MÜDAHALELERİN OLASI ETKİLERİ

Bitdefender kıdemli tehdit analisti Bogdan Botezatu'ya göre yazıcılar oldukça büyük bir güvenlik açığı oluşturmaktadır. "Güvenlik açığı değerlendirme laboratuvarlarımıza çok sayıda uzaktan ölçüm geliyor. Yönlendiriciler, artık internetteki en kötü aygıtlar değil. Yazıcılar onların yerini aldı bile."[3]

Bu güvenlik açığı, işletmeler üzerinde ciddi etkilere yol açabilir. Güvenli olmayan tek bir yazıcı yüzünden çok sayıda aygıtın bağlı olduğu ağınızı tamamen saldırılara açık bırakarak korsanların ağa bağlı aygıtlarınıza gizlice erişmesine olanak vermeniz ve tüm ağın güvenliğini tehlikeye atmanız söz konusu olabilir.

Güvenlik ihlallerinin etkilerine hepimiz şahit olduk. Spiceworks anketine katılanlar, bir ihlalin yol açtığı en önemli etkileri şöyle sıraladı:[1]

1. Yardım masası çağrısı ve destek sürelerinde artış

2. Üretkenlik/ verimlilikte düşüş

3. Sistem arıza süresinde artış

4. Destek çağrılarında harcanan sürede artış

5. Son kullanıcı politikalarının uygulanmasında artış

Ancak bir yazıcı ihlali, özellikle de yazdırılan verileri elektronik ortamda saklama özelliğine sahip çok işlevli bir yazıcı kullanıyorsanız, çok daha ciddi sonuçlara yol açabilir. Yazıcının önbelleğinde saklanan baskı işleri, korsanların hassas kişisel ve ticari bilgilere erişmesine olanak verir.

Daha da endişe verici olansa, korsanların güvenli olmayan bir yazıcı üzerinden geniş şirket ağına erişerek Sosyal Güvenlik numaraları, mali bilgiler veya şirket içi yazışmalar ve belgeler gibi bilgileri çalma olasılığıdır. Çalınan bu bilgiler, yalnızca bireysel olarak çalışanları etkilemekle kalmaz ve rakip şirketler tarafından veya şirketin itibarını zedelemek amacıyla kullanılabilir.

EN KOLAY ÇÖZÜM: DAHİLİ GÜVENLİK ÖZELLİKLERİ

Şirketlerin güvenlik konusunu tüm yazıcıları için ele alması gerektiği açıktır. Günümüzün modern kurumsal düzey yazıcılarında yazıcı tehditlerine karşı savunma sağlayan kullanımı kolay, dahili güvenlik özellikleri bulunmaktadır. Bu özelliklerden bazıları şunlardır:

- Saldırılara karşı otomatik algılama, koruma ve iyileştirme
- Yetkisiz kullanımı önlemek amacıyla izleme
- PIN veya akıllı kartlar gibi basit oturum açma seçenekleri
- Kullanıcıların yazıcıda yaka kartlarını kullanıp hızla kimliklerini doğrulayarak güvenle baskı almasını sağlayan proximity kart okuyucu
- Hassas belgeler için güvenli şifrelenmiş baskı özelliği

Bir sonraki masaüstü veya çok işlevli yazıcınızı satın alırken tümleşik güvenlik özelliklerine sahip olup olmadığına bakın ve bu özellikleri mutlaka etkinleştirin. Buna benzer yazıcılara özel, basit özellikler sayesinde yazıcılarınız üzerinden gerçekleşecek saldırılara karşı koruma elde edersiniz. Nesnelerin İnterneti yüzünden endişelenmeniz gereken onca erişim noktası varken, **yazıcıların bunlardan biri olmasına hiç gerek yok.**

DAHA GÜVENLİ YAZICILAR MI ARIYORSUNUZ?

DAHA FAZLA BİLGİ ›

Kaynaklar:

[1] Spiceworks tarafından HP adına Kuzey Amerika, EMEA ve APAC bölgelerinde 309 BT karar vericiyle gerçekleştirilen anket, Kasım 2016.

[2] "Printer Security: Is your company's data really safe?" *Computerworld,* 1 Haziran 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things on the Internet," *The Register*, 8 Eylül 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/