



Sponsor: **HP**

Yazarlar:

Angèle Boyd
Keith Kmetz
Matthew Marden

Kasım 2015

Yazıcı Güvenliğinin İş Değeri

IDC'NİN GÖRÜŞÜ:

IDC araştırması, görüşülen şirketlerin %80'inde BT güvenliğinin iş süreçleri açısından önemli olduğunu göstermiştir, ancak bu şirketlerin yalnızca %59'u baskı güvenliğinin iş süreçleri açısından önemli olduğunu belirtmiştir. Ayrıca üst yönetimin, baskı güvenliği yerine genel BT güvenliğine ilişkin karar alma sürecinde yer alması hemen hemen %40 daha olasıdır. Bu bulguların baskı güvenliğine yeterli önemin verilmediğini ve bunun da işletmeleri savunmasız bırakabileceğini gösterdiğine inanıyoruz. IDC araştırması, güvenli bir baskı ortamından aşağıdaki gibi önemli BT ve iş avantajları elde edildiğinden işletmelerin baskı güvenliğine daha fazla önem vermek için ikna edici nedenler olduğunu göstermiştir:

- » IDC tarafından gerçekleştirilen anket araştırması, görüşülen şirketlerin yarısından fazlasının son 12 ay içinde baskı güvenliğinin söz konusu olduğu bir BT güvenlik ihlali yaşadığını ortaya koymuştur.
- » Her kuruluşun baskı/belge ortamı güvenlik açıklarıyla doludur. Bu güvenlik açıkları, baskı aygıtlarının ve çıktıların dikkatsizce kullanımının yanı sıra kuruluş içinden veya dışından gelen kötü amaçlı saldırılardan kaynaklanabilir. Baskı ile ilgili potansiyel güvenlik ihlalleri, aygıtın ağ bağlantı noktaları, baskı/kopyalama/tarama işlerinin ele geçirilmesi, baskı/MFP sabit disk sürücüler ve belleği (RAM), çıkış tepsilerinde bırakılan basılmış veya kopyalanmış belgeler veya güvenli baskı malzemelerinin (çekler, reçeteler) yasadışı kullanımı vb. aracılığıyla gerçekleşir.
- » IDC'nin belirli bir düzeyde baskı ve ilgili belge iş akışı güvenliğine sahip kuruluşlarla yürüttüğü derinlemesine görüşmeler, baskı/belge güvenliğini benimseyen iki işletme türü olduğunu göstermiştir:
 - Güvenlik ve uyum çekinceleri ile kurum genelinde güvenli BT altyapısını benimseyen şirketler
 - Güvenlik girişimleriyle elde edilen maliyet ve BT verimlilikleriyle motive olan şirketler
- » Bir baskı güvenliği programını başlatmış olan kuruluşlarla IDC tarafından yürütülen görüşmeler, bu kuruluşların en önemli avantajları ve iş değerini üç alanda elde ettiğini göstermiştir:

Geliştirilmiş yazıcı güvenliği, BT personeli verimlilikleri ve maliyetlerin düşürülmesi. Görüşülen kuruluşlar baskı ve güvenlik ortamlarında aşağıdaki gibi etkileyici başarılar elde ettiklerini bildirmiştir:

- Yazıcı güvenliği çözümleri dağıtıldıktan sonra ortalama altı kat daha az yazıcıyla ilgili güvenlik ihlalleri yaşanması
 - Yazıcı güvenliği çözümleri dağıtıldıktan sonra personelin yazıcı ortamlarını desteklemesi için gereken sürenin ortalama yarı yarıya azaltılması
 - Kâğıt, toner ve mürekkep maliyetlerinde ortalama %15 tasarruf
- » Güvenlik çözümlerinin nasıl uygulandığı, yalnızca bu çözümlerin verimliliğini değil aynı zamanda çalışanların üretkenliğini de etkiler. Bu çözümlerden en yüksek faydayı sağlamak için teknolojiyle, çalışanlarla ve süreçlerle ilgili olarak göz önünde bulundurulması gereken önemli gereksinimler vardır.

Bu Teknik İncelemede

Bu teknik inceleme, IDC'nin BT ve baskıyla ilgili güvenlik açısından yürüttüğü birincil ve ikincil araştırmaya dayanmaktadır. IDC, Temmuz - Eylül 2015 arasında 16 kuruluşta baskı güvenliği çözümlerinin uygulanmasından ve yönetiminden sorumlu kişilerle derinlemesine görüşmeler gerçekleştirmiştir. Görüşmeler, IDC'nin kurumsal yazıcı güvenliği çözümleri kullanımının kuruluşlar üzerindeki nicel ve nitel etkilerini anlamasını sağlamak amacıyla tasarlanmıştır. Görüşmeler, çok çeşitli kuruluşların deneyimlerini yansıtmaktadır. 1. tabloda, görüşülen 16 kuruluşun baskı ortamlarına genel bakış sunulmaktadır.

TABLO 1

Görüşme Yapılan Kuruluşların Karakteristik Özellikleri — Derinlemesine Görüşmeler	Ortalama	Medyan	Aralık
Çalışan sayısı	60.300	20.500	200 - 290.000
BT personeli sayısı	4.500	610	40 - 25.000
BT kullanıcısı sayısı	57.200	19.500	180 - 290.000
Toplam yazıcı sayısı	8.800	1.200	4 - 100.000
Baskı alan kullanıcı sayısı	50.800	9.000	200 - 280.000
Yıllık basılan sayfa sayısı	51 milyon	10 milyon	10.000 - 300 milyon
Sektörler	Telekom, üretim, finans hizmetleri, yayıncılık, havacılık, biyoteknoloji, eğitim ve sağlık		

n = 16 kuruluş

Kaynak: IDC'nin Yazıcı Güvenliği Görüşmeleri, 2015

IDC, derinlemesine görüşmeleri anket çalışmasından elde edilen bulguların analiziyle tamamlamıştır. Uygun bulunan katılımcılar, tüm boyutlardan 440 kuruluştan gelen tam zamanlı çalışanlardır. Katılımcıların, şirkette kullanılan baskı güvenliği donanımlarının yanı sıra şirketin BT güvenlik politikaları hakkında bilgi sahibi olması şart koşulmuştur.

Duruma Genel Bakış

İşletmeler Baskı/Belge Altyapı Güvenliğine Neden Önem Vermelidir?

Birçok kuruluş, BT güvenliğini bir öncelik haline getirmiştir ve bunun geçerli nedenleri vardır. Bilgi işlem, mobil ve bulut teknolojilerinin ve diğer teknolojilerin yaygınlaşması, bilgi çalışanlarının iş bilgilerine "her zaman, her yerden" erişim ihtiyacı ve gereksinimi duydukları bir BT ortamını kolaylaştırmaktadır. Ancak IDC, baskı demirbaşlarının ve baskıyla ilgili teknolojilerin, bir kuruluşun BT güvenliği stratejisinin genelde göz ardı edilen unsurları olduğunu tespit etmektedir.

Peki, işletmeler baskı güvenliğine olan mevcut yaklaşımlarını neden değiştirmeli ve diğer teknolojilerde (bilgisayarlar, sunucular, mobil aygıtlar vb.) olduğu gibi baskı aygıtlarını da neden güvence altına almalıdır? Çünkü güvenli olmayan bir baskı altyapısı, genel olarak güvenli olmayan bir BT ortamı demektir. Yazıcıyla ilgili güvenlik ihlalleri yaşanması riski beklenenden yüksektir ve maliyetli yükümlülükler söz konusudur.

IDC anket araştırması, geçen 12 ayda şirketlerin yarısından fazlasının baskı güvenliği de dâhil olmak üzere bir BT güvenlik ihlali yaşadığını ortaya koymuştur. Bu güvenlik açıkları, baskı aygıtlarının ve çıktıların dikkatsizce kullanımının yanı sıra kuruluş içinden veya dışından gelen kötü amaçlı saldırılardan kaynaklanabilir. Baskı ile ilgili potansiyel güvenlik ihlalleri, ağ bağlantı noktaları, baskı/kopyalama/tarama işlerinin ele geçirilmesi, baskı/MFP sabit disk sürücüler ve belleği (RAM), çıkış tepsilerinde bırakılan basılmış veya kopyalanmış belgeler, güvenli baskı malzemelerinin (çekler, reçeteler) yasadışı kullanımı vb. aracılığıyla gerçekleşir. Ayrıntılar:

- » Güvenli olmayan ağ bağlantı noktaları, şirket ağına ve bilgi varlıklarına giriş noktasıdır.
- » Gizli belgelerin (örn. hasta bilgilerinin veya müşteri mali işlemlerinin yer aldığı belgeler) paylaşılan yazıcılarda basılması ve bu belgelerin bir süre çıkış tepsilerinde kalması, gizli bilgilerin çalınması ve yasal uyumluluk sorunları yaşanması için bir fırsat oluşturur.
- » Şifrelenmemiş baskı/tarama verilerinin iletilmesi, bilgisayar korsanlarına davetiye çıkarmak gibidir.

IDC anket araştırması, geçen 12 ayda şirketlerin yarısından fazlasının baskı güvenliği de dâhil olmak üzere bir BT güvenlik ihlali yaşadığını ortaya koymuştur.

Güvenlik ihlalleri maliyetlidir. Üç tür potansiyel mali yükümlülük bulunmaktadır:

- » **İhlali çözmeye yönelik olarak kullanılan şirket kaynakları.** Bir güvenlik ihlali yaşayan şirketler, olayı "düzeltmek" için önemli çalışan zamanı ve maliyetleri kullanır. Bu olayla ilgilenmek için potansiyel gelir getiren fırsatlar ertelenir veya iptal edilir.
- » **Para cezaları/cezalar.** Şirketler, uyumsuzluk (örn. HIPAA) veya müşteri gizliliğinin ihlaline ilişkin davalar nedeniyle mali cezalarla karşılaşabilir.
- » **Şirket itibarı.** Kuruluş, bir olay sonucunda basında çıkan kötü haberlerle lekelenmiş itibarı nedeniyle mali olarak zarar görmeye devam edebilir.

Baskı Altyapısı Güvenliği için Tetikleyiciler

Çeşitli düzeylerde baskı güvenliği kullanan kuruluşlarla gerçekleştirilen derinlemesine görüşmelere dayanarak uygulamaları için aşağıdaki tetikleyicileri tespit ettik:

- » Güvenlik ve uyumluluk endişeleri (bir ihlale müdahale edilmesi dâhil)
- » BT altyapısı genelinde proaktif güvenlik standardizasyonu
- » Maliyet tasarrufları ve BT verimlilikleri

Güvenlik ve Uyumluluk Çekinceleri

Fikri mülkiyet (IP), gizli veya sınırlandırılmış bilgiler, yasal uyumluluk ile ilgili güvenlik çekinceleri ve kurum genelinde tutarlı, güvenli BT altyapısı ihtiyacı, baskı güvenliği programı için önemli etmenlerdir. Bazı kuruluşlar, geçmiş olaylara veya ihlallere yanıt olarak daha güçlü baskı güvenliği programları kullanmaktadır.

Bir finans hizmetleri şirketinin üst düzey sistem direktörü konuyla ilgili şunları söyledi: "Güvenlik çekinceleri her yerde mevcuttur ve yazıcılar gizli, sınırlandırılmış veya gizli olmayan kullanım için genel olarak erişilebilir aygıtlardır. Gizli/sınlandırılmış verilerle ilgilenen tüm ağ aygıtları güvenlik, uyumluluk ve denetim gereksinimlerine tabidir; bu nedenle bunu yapmak zorunda kaldık."

BT Altyapısı Genelinde Standardizasyon

Bir kuruluşun genel BT altyapısında güvenlik standardizasyonu, bu donanımın kullanımıyla ilgili sorunların çözülmesine yönelik kapsamlı bir politikanın yanı sıra baskı ve ilgili belge güvenliğinin benimsenmesini de teşvik eder. Bir yayıncılık şirketinin bilgi teknolojisi başkan yardımcısı şu açıklamayı yaptı: "Bir politikaya tabi olarak yürütülen güvenlik, sorunların

Fikri mülkiyet (IP), gizli veya sınırlandırılmış bilgiler, yasal uyumluluk ile ilgili güvenlik çekinceleri ve kurum genelinde tutarlı, güvenli BT altyapısı ihtiyacı, baskı güvenliği programı için önemli etmenlerdir.

Maliyet tasarrufları, güvenli bir baskı ve ilgili belge güvenliği planını izlemenin sağladığı dolaylı ancak önemli avantajlardan biridir.

otomatik çözümü ve [yazıcılar için] kimlik belgelerinin diğer altyapı hizmetlerine olan yaklaşımımızla tutarlı olduğu bir altyapı güvenliği istedik.”

Maliyet Tasarrufları ve BT Verimlilikleri

Bir kuruluşun işletme maliyetlerinin azaltılmasına yardımcı olan bir BT girişi, üst yönetime cazip gelir. Maliyet tasarrufları, güvenli bir baskı ve ilgili belge güvenliği planını izlemenin sağladığı dolaylı ancak önemli avantajlardan biridir. Bu avantaj, bir baskı ve belge güvenliği programını benimsemenin başlıca etmeni olmasa da yarattığı etki, anket çalışmasına katılanların üçte biri tarafından fark edilmiş en önemli avantajdır.

Bir finans hizmetleri şirketinin üst düzey BT direktörü şu açıklamayı yaptı: “Fikri mülkiyeti koruma ihtiyacı ve veri güvenliğiyle ilgili potansiyel mali etkiler, bu çözümlerin neden uygulandığının temelini oluşturmuştur ... düşüncesizce ve gereksiz bir şekilde baskı alınmasını sınırlayan denetimlerin hem kâğıt hem de malzeme maliyetlerinde tasarruf sağladığından son derece eminiz.”

Elbette ki baskı güvenliği girişi aracılığıyla elde edilen “daha az doğrudan” maliyet tasarrufu avantajları bulunmaktadır. Birçok kuruluş, baskı ve güvenlik yönetiminin merkezileştirilmesi ve standardizasyonu yoluyla elde edilen BT verimliliklerinin maliyet avantajları sunduğuna dikkat çekmektedir. Baskının daha etkin bir şekilde yönetilmesi ve güvenceye alınması BT’nin, kuruluşun diğer öncelikli teknoloji ihtiyaçlarıyla ilgilenmek için serbest kalmasını sağlar. Örneğin, bir üniversitenin BT direktörü şu açıklamayı yaptı: “Baskı ortamımız üzerindeki maliyet denetimini ve merkezi yönetim denetimini birleştirmek istiyoruz.”

Yazıcı Güvenliğinin İş Değeri

IDC’nin kurumsal yazıcı güvenliği çözümlerini kullanan 16 kuruluşla gerçekleştirdiği derinlemesine görüşmeler, söz konusu kuruluşların bu çözümleri kullanarak önemli iş değeri elde ettiğini ortaya koymuştur. IDC’nin kuruluşlardan yazıcı güvenliği çözümlerini uygulamadan önceki ve sonraki yazıcı ortamlarını açıklamalarını istediği bu görüşmeler, söz konusu kuruluşların yazıcı güvenliği maliyetleri ve personel süreleri konusunda verimliliklerini sürdürürken daha güvenli baskı ortamları oluşturma hedeflerine de ulaştıklarını göstermiştir.

- » **Güvenlik.** Yazıcı ortamları daha güvenli hale getirilmiş ve veri ihlallerini düzeltme, yasal uyumluluk ve denetim uyumluluğu sağlamakla ilgili maliyetler düşürülmüştür.
- » **BT personeli verimlilikleri.** Yazıcı ortamlarını yönetmek ve devam ettirmek, yazıcılarla ilgili bir politika oluşturmak, bu politikayı değiştirmek ve uygulamak için gerekli personel süresi azaltılarak personelin diğer girişimler üzerinde çalışması için zaman kazandırmıştır.

Bu kuruluşlar, kurumsal yazıcı güvenliği çözümlerini uygulamaya başladıklarından beri yazıcılarla ilgili güvenlik ihlalleri yaşanma sıklığının ortalama olarak altı kata kadar azaldığını bildirmiştir.

- » **Maliyet tasarrufları.** Baskıyla ilişkili maliyetler, gelişmiş görünürlük ve değiştirilen baskı davranışı ile yazıcılar ve yazıcı sarf malzemeleri açısından sağlanan tasarruflar da dâhil olmak üzere düşürülmüştür.

Risk Azaltma: Geliştirilmiş Yazıcı Güvenliği ve Uyumluluğu

Görüşülen kuruluşlar, yazıcıyla ilgili güvenlik ihlallerinin etkisini azaltmak ve uyumluluk çalışmalarını daha verimli ve daha uygun maliyetli bir hale getirmek için kurumsal yazıcı güvenliği çözümlerinin kullanımını geliştirdiklerini bildirmişlerdir.

IDC, derinlemesine görüşmelere katılanlara yazıcıyla ilgili güvenlik ve veri ihlallerinin kuruluşlarında gerçekleşme sıklığını ve kuruluşlarının yazıcıyla ilgili önemli güvenlik ihlalleri yaşayıp yaşamadığını sormuştur. Bu kuruluşlar, kurumsal yazıcı güvenliği çözümlerini uygulamaya başladıklarından beri yazıcılarla ilgili güvenlik ihlalleri yaşanma sıklığının ortalama olarak altı kata kadar azaldığını bildirmiştir. Baskı işlerinin şifrelenmesi, kullanıcı kimlik doğrulaması ve kimlik doğrulamalı baskı uygulamaları, güven veren ve ihlallerin önlenmesine yardımcı olan bir düzeyde izlenebilirlik ve sorumluluk sağlamıştır. Ayrıca yazıcı güvenliği, bazı kuruluşların BT altyapıları genelindeki güvenlik girişimlerini tamamlamalarına; dolayısıyla, geri kalan güvenlik açıklarını kapatmalarına yardımcı olmuştur. Görüşülen şirketler, yaşamış oldukları yazıcıyla ilgili güvenlik ihlallerine aşağıdaki gibi örnekler sunmuşlardır:

- » **Gizli bilgilerin kötü amaçlı kullanım niyetiyle basılması.** Bir üretim şirketinin BT direktörü, diğer unsurların yanı sıra çalışanların gizli ve özel bilgileri basmalarının ve bu bilgileri şirketin rakiplerine sunmalarının bir sonucu olarak kuruluşunun fikri mülkiyet kaybı yaşadığını açıklamıştır.
- » **Güvenli bilgilerin basılması ve kötüye kullanılması.** Bir finans hizmetleri şirketinin BT direktörü, kuruluşundaki çalışanların rasgele baskı alarak veya baskı işlerini yazıcıda bırakarak tasarımları ve diğer fikri mülkiyetleri riske attıklarını açıklamıştır.

Görüşülen kuruluşlar, kurumsal baskı güvenliği çözümlerinin, yazıcılar aracılığıyla gerçekleşen güvenlik ihlallerinin etkisini en aza indirmelerine nasıl yardımcı olduğuna ilişkin çeşitli örnekler vermiştir:

- » **Baskı süreci boyunca bilgilerin korunması.** Bir yayıncılık şirketinin bilgi teknolojisi başkan yardımcısı şu açıklamayı yaptı: "Çözüm, ağ üzerinden yazıcılarımıza giden veya yazıcılarımızdan gelen içerik ve veri iş akışını korumak için çok önemli bir araç olmuş, güven ortamı sağlamış ve ihlallere yönelik fırsatları azaltmamıza yardımcı olmuştur."

» **Gereksiz veya uygunsuz baskı almayı önleme.** Bir finans hizmetleri şirketinin BT direktörü şunları söyledi: “Genelde kurum içinde dağıttığımız gizli belgeler asla basılmamalıdır. Bu çözümler, giderek artan bir kısmı kasıtlı olarak veya rasgele baskı almanın bir sonucu olarak kurum içinde meydana gelen ihlalleri en aza indirmemize yardımcı olur.”

2. tabloda, yazıcılarla ilgili tüm güvenlik ihlallerinin maliyetli olabileceğini, ancak kuruluşların önemli güvenlik ihlallerinden kaçınmasının, bu ihlallerin yol açtığı ciddi maliyetler nedeniyle özellikle önem taşıdığını gösterilmektedir. Son yıllarda yazıcıyla ilgili önemli olarak tanımladıkları bir güvenlik ihlali yaşamış olan beş şirketle yapılan görüşmelere göre önemli bir güvenlik ihlalinin ortalama maliyetleri, 54 çalışan için üretkenlik kayıplarını, 277 saat düzeltme süresini ve para cezaları da dâhil olmak üzere ihlal başına 500.000 \$ üzerinde bir maliyeti içermektedir.

TABLO 2

Kurumsal Yazıcı Güvenliği Çözümlerinin Güvenlik İhlalleri Üzerindeki Etkisi — Derinlemesine Görüşmeler

Genel olarak güvenlik ihlalleri

Yıllık ihlallerin ortalama sayısı — yazıcı güvenliği uygulanmadan önce	9,9
Yıllık ihlallerin ortalama sayısı — yazıcı güvenliği ile	1,5
Güvenlik ihlallerinin sayısında değişiklik	6 kata kadar daha az

Önemli güvenlik ihlalleri

Görüşülen kuruluşlar arasında önemli güvenlik ihlalleri yaşayan kuruluşların sayısı	5
Etkilenen çalışanların ortalama sayısı	54
Çözmek için gerekli olan ortalama çalışan süresi (saat)	277
İhlal başına düşen düzeltmenin toplam ortalama maliyeti (para cezaları dâhil)	521.400 \$

n = 16 kuruluş

Kaynak: IDC'nin Yazıcı Güvenliği Görüşmeleri, 2015

Yazıcıyla ilgili güvenlik ihlalleri sıklığının azaltılmasına ek olarak görüşülen 16 şirketin 10'u yasal uyumluluklarını ve denetim çalışmalarını daha etkili ve daha verimli kılmak için yazıcı güvenliği çözümlerine yatırım yapmıştır. Geliştirilmiş güvenlik ve izlenebilirlik şu avantajları sağlar:

- » **Geliştirilmiş güvenlik:** Bir finans hizmetleri şirketinin sistem direktörü şunları söyledi: "Bu güvenlik modelinin uygulanmasının merkezinde, verileri ve belgeleri koruyan, tasarım ve mimari gizliliğini artıran çok sağlam ve güvenli bir ortam oluşturmak için elde ettiğiniz avantaj bulunmaktadır ve yazıcılarının güvenliğini sağlamak, güvenlik standartlarımızı karşılamamıza önemli ölçüde yardımcı olmuştur."
- » **İzlenebilirlik ve görünürlük:** Bir yaşam bilimleri şirketinin BT başkan yardımcısı şu açıklamayı yaptı: "Bir denetim kaydı oluşturduk, verilerin durdurulmasını engelledik ve gizli verilere sınırlandırılmış kullanıcı erişimimiz olduğunu gösterdik. Ayrıca doğrulama ve denetim sürecimiz, risk belirleme ve tehdit analizi ve sorunları gidermeye yönelik önerilen düzeltmeleri içermektedir. Sistem durumuna ayrıntılı bir genel bakış sağlarız ve gerçek zamanlı izleme gerçekleştirebilir, uyumluluk için tüm gereksinimleri karşılayabiliriz."

Bu iyileştirmeler ayrıca kuruluşların uyumluluk ve denetim çalışmaları için zaman ve maliyet tasarrufları sağlamıştır. Ortalama olarak görüşülen şirketler, yazıcı güvenliği çözümlerini kullanımlarının kendilerine yıllık 200 saatin üzerinde bir çalışan süresi kazandırdığını, denetim ve uyumluluk için üçüncü taraf destek maliyetleri de dâhil olmak üzere ilgili maliyetlerde yıllık neredeyse 250.000 \$'a varan bir tasarruf sağladığını bildirmiştir.

BT Personeli Üretkenlik Avantajları

IDC'nin görüştüğü kuruluşlar, yazıcı güvenliği çözümlerini uygulamaya başladıklarından beri yazıcı güvenliklerini yönetmek ve desteklemek için gereken zaman yükünü azalttıklarını bildirmiştir. Bu verimlilikler, yazıcıyla ilgili sorunların daha hızlı çözülebilmesinin yanı sıra merkezileştirilmiş yönetim özellikleri ve otomasyon kullanıma alınması veya yaygınlaştırılması gibi etkenlerle sağlanmaktadır. Bir finans hizmetleri şirketinin üst düzey BT direktörü şu açıklamayı yaptı: "Hem zaman alan faaliyetlere harcanan saatler hem de ekibin daha stratejik faaliyetlere odaklanmasını sağlama bakımından [yazıcı güvenliği çözümlerinin uygulanmasını] personel üzerinde büyük etkisi olmuştur. Yazıcıyla ilgili sorunlara verilen yanıt bundan böyle kopuk değil, bütüncül ve tekrarlanabilir özelliktedir." Sonuç olarak görüşülen kuruluşlar, IDC'ye yazıcı güvenliği çözümlerini uygulamaya başladıktan sonra personelin yazıcı ortamlarını desteklemesi için gerekli olan süreyi yarı yarıya azalttıklarını söylemiştir.

Görüşülen şirketler, yazıcı güvenliği çözümlerinin yazıcı ortamlarından sorumlu personel için verimlilikler sağladığını bildirmiştir. Personel süresi tasarrufları, kapsamlı belge otomasyonu da dâhil olmak üzere destek ve bakım otomasyonu ve diğer tekrarlanabilir süreçlerin uygulanması gibi değişikliklerden kaynaklanır. Örneğin, benzersiz belge ve çalışan kimlik doğrulama politikaları uygulayan bir finans hizmetleri şirketinin başkan yardımcısı, kuruluşunun personelin aygıtları izlemek için harcadığı süreyi %60 oranında nasıl azalttığını açıkladı: "Profiller

Sonuç olarak görüşülen kuruluşlar, IDC'ye yazıcı güvenliği çözümlerini uygulamaya başladıktan sonra personelin yazıcı ortamlarını desteklemesi için gerekli olan süreyi yarı yarıya azalttıklarını söylemiştir.

kolaylıkla oluşturulabildiği, birçok ağıta eş zamanlı olarak gönderilebildiği ve sertifika yönetimini otomatikleştirebildiğimiz için BT personeli çalışma süresinden tasarruf ediyor.”

Bu arada görüşülen kuruluşlar, yazıcıyla ilgili politikaların oluşturulmasında, uygulanmasında ve değiştirilmesinde yazıcı güvenliği ile sağlanan zaman tasarruflarından da yararlanmaktadırlar. Ortalama olarak bu kuruluşlardaki personel, yazıcıyla ilgili politikaya %59 daha az zaman harcar. Personel süresi tasarruflarının ötesinde yazıcıyla ilgili politikanın daha etkili uygulanması, ihlallerin olasılığını azaltma ve yazıcı kullanımına yönelik daha etkili yönergeler oluşturma gibi avantajlar sunar.

Görüşülen kuruluşlar, yazıcılarla ilgili sorunlar ortaya çıktığında personelin yazıcı güvenliği çözümlerinin merkezi konsollar ve yazıcılara uzaktan erişim gibi özelliklerinden yararlandığını (veya daha iyi bir şekilde geliştirdiğini) bildirmiştir. Bu etkenler, görüşülen kuruluşların, yazıcıyla ilgili geliştirilmiş politikaya ek olarak yazıcıyla ilgili olaylara ve yazıcı kullanıcılarından gelen yazıcıyla ilgili çağrılara yanıt vermeleri için gereken süreyi ortalama olarak sırasıyla %59 ve %42 oranında azaltmasına yardımcı olmuştur (bkz. Şekil 1). Otomatik düzeltme ve yönetilen benzersiz sertifikaları içeren güvenlik çözümlerini kullanan bir yayıncılık şirketinin BT başkan yardımcısı, bu çözümlerin ekibinin yazıcıları destekleme becerisi üzerindeki etkisini şöyle açıkladı: “Artık daha az sorun var ve şu anda mevcut olan sorunların giderilmesi daha az zaman alıyor. Olumlu olan söz konusu etki, diğer destek ve planlama faaliyetleri için zaman sağlıyor.” Yazıcı güvenlik yönetimi ürünü kullanan bir finans hizmetleri şirketinin BT direktörü şunları söyledi: “Yardım masamızın, yazıcı ayarları, izinler ve sorunlar konusunda artık net bir görüşü var ve düzey 2 desteği için bağımsız hareket edebilirler veya küçük bir kurumsal baskı ekibiyle iletişime geçebilirler.”

ŞEKİL 1

Ortalama Yazıcıyla İlgili Personel Çalışma Süresi Tasarrufları — Derinlemesine Görüşmeler



n = 16 kuruluş

Kaynak: IDC'nin Yazıcı Güvenliği Görüşmeleri, 2015

Baskıyla İlgili Maliyetlerin Azaltılması

Aynı zamanda maliyetleri azaltan tüm temel BT girişimleri daha caziptir. Sonuç olarak, görüşülen kuruluşların yazıcı güvenliği çözümlerini uygulama yoluyla maliyet tasarrufları sağlayabilmeleri önemli bir katma değer oluşturmuştur. Çalışan kimlik doğrulaması ve kimlik doğrulamalı baskı gibi uygulamalar, derinlemesine görüşme yapılan katılımcılar tarafından en çok kullanılan uygulamalar arasında yer almıştır (görüşülen kuruluşların üçte ikisinden fazlası kullanmaktadır). Bu çözümler, yazıcı kullanıcılarının belge basmak için doğrulayıcı aşamalardan geçmelerini gerektirerek ve sahipsiz veya yanlış yönlendirilmiş baskı işlerinin sayısını azaltarak belge gizliliğini korur ve maliyet tasarrufları sağlar. Yazıcı güvenliği çözümlerinin yazıcıyla ilgili maliyetleri azaltma aracı olarak kullanılabilmesi, görüşülen birçok kuruluşun maliyetlerin en iyi duruma getirilmesini, yazıcı güvenliği çözümlerini kullanmalarının başlıca etmeni olarak görmelerinden net bir şekilde anlaşılmaktadır.

Görüşülen kuruluşlar, yazıcı güvenliği çözümlerinin maliyetleri azaltmalarına yardımcı olduğunu açıklamıştır:

- » **Baskı alma davranışını değiştirip baskı miktarını azaltarak:** Gıda endüstrisindeki bir şirketin kurumsal hazine sorumlusu şunları söyledi: "Kullandığımız kimlik doğrulamalı baskı özelliği, belgeleri baskıya göndermenize izin verir, ancak bunları gerçekten basmak için gidip yaka kartınızı yazıcıya okutmanızı gerektirir. Gördüğüm son rakamlara göre sanırım çıktılarda daha öncesine kıyasla %21 ile %24 arasında bir azalma sağladı."
- » **Yazıcı kullanımına görünürlük kazandırarak:** Bir üniversitenin BT direktörü şunları söyledi: "Artık departmanlardan ücret talep edebilmek için basılan sayfaların maliyet takibini yapabiliyoruz." Baskı maliyetlerini departman bazında değerlendirebilen üniversite, yazıcı kullanıcılarını mümkün olduğu kadar verimli hale getirme yöntemlerini bulma sorumluluğunu her bir departmana verebilir.
- » **Gereksiz veya eski yazıcıları kullanımdan kaldırarak:** Bir finans hizmetleri kuruluşunun başkan yardımcısı şunları söyledi: "Arkadaşlarımız baskı faaliyetinin izlendiğini bildikleri ve kurumsal baskı güvenliği temellerini desteklemeyen eski baskı donanımlarını kullanımdan kaldırdığımız veya değiştirdiğimiz için gereksiz baskı işlerinin sayısını azaltıyoruz."

Yazıcı güvenliği girişimleri, daha fazla baskı işi alan çalışanların yazıcı kullanımı hakkında daha bilinçli olmalarını sağlamış ve yazıcıyla ilgili maliyet tasarruflarına katkıda bulunmuştur. Derinlemesine görüşme yapılan katılımcılar ortalama olarak çalışanların yanlış yazıcıya %43 daha az baskı işi gönderdiğini söylemiştir. Sonuç olarak, daha az baskı işi sahipsiz bırakılmış veya tekrarlanmıştır. Şekil 2'de gösterildiği gibi bu iyileştirme tipleri, daha az genel baskı (ortalama olarak %6 azalma), daha fazla çift taraflı baskı (%19 artış) ve biraz daha az renkli baskı (%2 azalma) yapılmasını sağladığı gibi genel olarak daha verimli yazıcı kullanımına katkıda bulunmuştur. Bu etkenler, yazıcı ortamlarına gelişmiş bir görünürlük kazandırmanın yanı sıra görüşülen kuruluşların, kullandıkları ve bakımını yaptıkları yazıcı sayısı da dâhil olmak üzere (%1 azalma veya kuruluş başına ortalama 115 yazıcı) baskı ortamlarında ve kâğıt, mürekkep

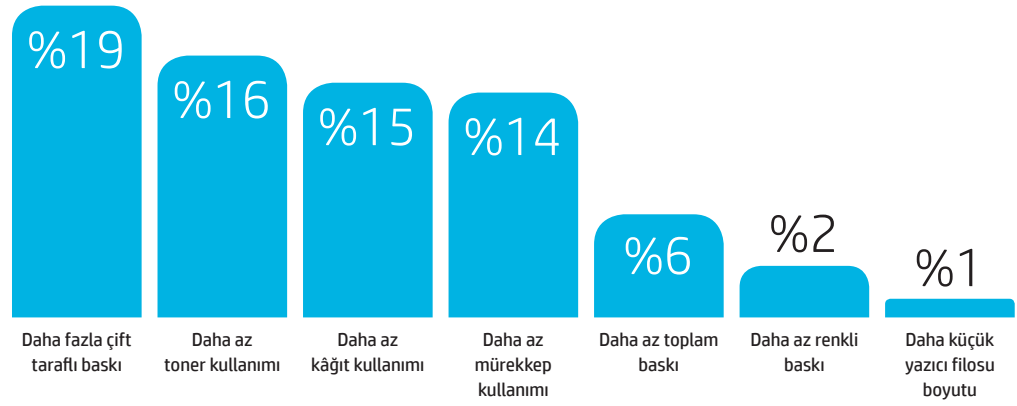
Yazıcı güvenliği girişimleri, daha fazla baskı işi alan çalışanların yazıcı kullanımı hakkında daha bilinçli olmalarını sağlamış ve yazıcıyla ilgili maliyet tasarruflarına katkıda bulunmuştur.

ve toner ile ilişkili maliyetlerde önemli tasarruflar (sırasıyla %15, %14 ve %16) elde etmelerini sağlamıştır.

ŞEKİL 2

Ortalama Yazıcı Ortamı Maliyet Tasarrufları ve Yazıcı Verimlilikleri — Derinlemesine Görüşmeler

(% verimlilik veya iyileştirme)



n = 16 kuruluş

Kaynak: IDC'nin Yazıcı Güvenliği Görüşmeleri, 2015

Karşılaşılan zorluklar

Hemen hemen her kuruluşta yeni bir uygulamaya başlamadan planlama yapmak yoluyla bazı zorluklar önceden önenebilir. Çalışma grubunun zorlukları, baskı güvenliğinin uygulamaya alınmasının üç aşamasına da yayılmıştır: planlama, uygulama ve uygulama sonrası.

İncelenen şirketler, strateji ve plan geliştirmek için kendilerini zaman baskısı altında hissettiklerini bildirmiştir. Uygulama sonrasında BT'nin iş yükünde azalma sağlamak için daha önceden bu konuya önemli bir süre ayırmak gerekir. Ayrıca çalışan uyumluluğunun sağlanması, izleme araçlarını, bir eskalasyon sürecini ve baskıyla ilgili yardım masası çağrılarını azaltmaya yönelik düzeltmeleri kapsayan otomatikleştirilmiş bir süreç olmalıdır.

Bir kuruluşun yazıcı kullanıcıları için planlanması gereken iki noktaya dikkat çekiyoruz:

- » **Çalışan üretkenliğinin olumsuz etkilenmesini en aza indirirken sıkı baskı güvenliğinin dengelenmesi:** İş güvenliğinin en yüksek öneme sahip olması gerekir, ancak bir kuruluş, üretkenlik üzerinde en az olumsuz etki yapacak bir sistem üzerinde çalışmalıdır. Örneğin, baskı güvenliği ihtiyaçlarına yönelik olarak kimlik doğrulamalı baskı özelliğini uygulayan bazı kuruluşlar, kimlik doğrulaması (parola girmek gibi) ve ardından tüm belgenin basılmasını bekleme gerekliliği nedeniyle kullanıcı direnciyle karşılaşabilir. Bu

IDC, bir kuruluşun baskı/belge güvenliği teknolojisini sarsılmaz hale getirmesini önerir.

senaryodaki denge unsuru, belgede bulunan bilgilerin korunmasına (örn. kâğıt tepesinde başıboş bırakılmış belgeleri kimse göremez) karşılık bir belgenin basılmasını beklemektir (örn. baskı işlemi ancak kullanıcı aygıtta kimlik doğrulamasını gerçekleştirdikten sonra başlatılır).

- » **Çalışan eğitimi:** Çalışan üretkenliğiyle ilgili olarak baskı güvenliği planı, çalışanları yeni politikalar ve yordamlar konusunda eğitmek için gerekli olan süreci ve zamanı içermelidir. İşletmeler, tekrarlanan eğitimler vermeye ve çalışanların arasındaki nesil ve öğrenme tarzı farklılıklarına uygun olan farklı formatlar kullanmaya hazırlıklı olmalıdır.

Temel Kılavuz

IDC, yazıcı ve ilgili belge iş akışlarını kuruluş genelindeki BT güvenliği çerçevesine dâhil etmek için birçok ikna edici neden belirlemiştir. Açıkçası temel avantajlardan biri, baskıyı içeren kapsamlı bir BT güvenliği programının sağlanmasına tabidir, ancak bu tür bir planın güvenliğinin ötesinde birçok önemli avantajı vardır. İki önemli avantaj, belirgin maliyet tasarrufları ve artırılmış BT verimliliğidir.

IDC, bir kuruluşun baskı/belge güvenliği teknolojisini sarsılmaz hale getirmesini önerir. Kuruluş, yalnızca çalışanlar ve süreçler planının yürütülmesine dâhil edildiğinde bu hedefin etkili bir şekilde gerçekleştirilebileceğini bilmelidir.

Teknoloji

Güvenlik açısından teknoloji çözümlerinin uygulanması temelde siyahla beyaz gibidir... bir kuruluş ya güvenlidir ya da güvenli değildir.

IDC, aşağıdaki becerilerin mümkün olan en kısa sürede kuruluş genelinde uygulanmasını önerir. BT personeli ve baskı altyapısı sağlayıcıları, aşağıdaki özelliklerin ve becerilerin yapılandırılmasını ve kuruluş genelinde kullanılan tüm baskı aygıtları için etkin olmasını sağlamalıdır:

- » Tüm ağa bağlı baskı aygıtlarının aşağıdaki özelliklere sahip olduğundan veya en azından ürün yazılımlarının bu özellikleri yansıtacak şekilde yükseltildiğinden emin olunması.
- » Aygıtların yalnızca şifrelenmiş iletişim protokollerini kullandığından ve geri kalan protokoller devre dışı bıraktığından emin olunması.
- » Aygıtın kullanımdan çıkarılmasının bir parçası olarak aygıtın sabit disk sürücüsü verilerini silen veya yok eden bir sistemin uygulamaya koyulması.
- » En az bir (tercihen iki veya üç) kullanıcı kimlik doğrulaması biçiminin desteklenmesi ve yüksek hacimli gizli bilgilere veya uyumluluk gereksinimlerine yönelik kimlik doğrulamalı baskı uygulamasının baskı ortamları için değerlendirilmesi.

- » Ürün yazılımının güncel olduğundan ve yalnızca yasal ürün yazılımının yüklü olduğundan emin olunması.
- » Tüm yazıcı sabit disk sürücülerinin güvenli olduğundan emin olunması (verilerin düzenli olarak şifrelenmesi ve silinmesi).
- » Kuruluşun çıktıları gerektiyorsa, özel baskı malzemeleri için kurcalanmaya karşı dayanıklı baskı özelliklerinin uygulanması veya kilitli çekmeceli yazıcılar kullanılması. Bu uygulama çekler, reçeteler gibi dolandırıcılık için potansiyel hedef olan çıktılarının güvenliğini sağlayacaktır.
- » Güvenlik politikalarına uyum sağlamak amacıyla aygıtın merkezi olarak yönetilmesi, izlenmesi ve iyileştirilmesi için bir filo yönetim aracının kullanılması. Böylece kuruluş, her bir aygıtı ayrı ayrı yapılandırmak ve her bir aygıtın bakımını yaptırmak zorunda kalmaz. Araç, güvenlik politikasının basit/kolay bir şekilde oluşturulmasına ve yönetilmesine olanak sağlamalı, ağa aygıtlar eklendiğinde bunu algılamalı, benzeriz aygıt sertifikası yönetimi sağlamalı ve uyumsuz olayları kaydetmeli ve eskalasyon ve düzeltme süreci aracılığıyla olayları çözmelidir. Araç, uyumsuz olaylar ve anormallikler için son noktaları izleyen kurum genelindeki BT güvenlik yönetimi araçlarıyla birlikte çalışmalıdır, böylece tüm potansiyel güvenlik ihlalleri hızlı bir şekilde belirlenebilir.
- » Hem masaüstü hem de mobil aygıt baskılarının ve taramalarının (hareket halinde veya sabit durumda), baskıyla ilgili verilerin tam olarak korunabilmesi için şifrelendiğinden emin olunması. Bu durum, ek koruma için basılacak eklerin bile açılması ve görüntülenmesi gerektiği anlamına gelir. Baskı ve tarama içeriğini izleyen bir araç, en yüksek güvenlik düzeyini ve belirlenmiş şirket standartlarına uyum sağlamak için önemli bir unsurdur.

Çalışanlar

BT güvenliği ihtiyaçlarını ciddiye alan bir kuruluş, güvenlik ekibinde baskı aygıtlarının ve ilgili belge iş akışlarının güvenliğinin sağlanmasında vasıflı personelin bulunduğundan emin olmalıdır. Bu güvenlik ekibi, kuruluşun kendi kurum içi personelinden ve/veya harici güvenlik kaynaklarından oluşabilir. Ekipten gelecek baskı ve iş akışı güvenliği konularında tavsiye vermesi ve bir BT güvenlik planının kurum genelinde bütünleştirilmesine yardımcı olması talep edilecektir.

Kuruluş, baskı aygıtları ve ilgili belge iş akışları güvenliğinin sağlanmasının çalışan üretkenliğini olumsuz etkilemediğinden emin olmak için planlama sürecinin bir parçası olarak belirli çalışanlardan bilgi almalıdır. Gerekli değişikliklerin miktarı veya niteliği önemliyse bir değişiklik yönetimi uzmanının sürece dâhil edilmesi de önerilir. Söz konusu uzman, kullanılacak olan uygulamaya alma ve eğitim yaklaşımı konularında da tavsiyede bulunabilir.

Kuruluşların çoğu baskı ve belge altyapılarının güvenliğini kendi kendilerine sağlamak için gerekli bilgi birikimine ve becerilere sahip değildir. Bu nedenle bir kuruluş, BT departmanının geliştirebileceği kaynaklar hakkında baskı aygıtı sağlayıcısına danışmayı düşünmelidir. Kaynaklar, bir kuruluşun yazıcı/MFP donanımında bulunan güvenlik özelliklerini, güvenlik yazılım araçlarını ve güvenlik hizmetlerini (örn. güvenlik profesyonel hizmetleri, güvenlik değerlendirmeleri, değişiklik yönetimi ve belirli sektörlerde yasal uyumluluk uzmanlığı) kapsamaktadır.

Süreç

Bir kuruluşun kendi güvenlik girişimini, baskı ortamının güncel durumunu değerlendirerek başlatması ve geri kalan BT ortamının güvenlik düzeyiyle tutarlı bir güvenlik düzeyi sağlayan bir plan geliştirmesi önemlidir. Bu girişim, kuruluşun faaliyet gösterdiği sektöre özgü temel güvenlik gereksinimlerini karşılamanın yanı sıra bu politikaları devamlılık arz eden bir şekilde izleme, eskalasyon, düzeltme ve uygulama için bir plan içermelidir.

Plan, düzenlemelerin gerekli olup olmadığını belirlemek ve şirket dışındaki baskı/belge ihlallerinden ders çıkarmak için toplanan veriler kullanılarak düzenli bir şekilde yeniden değerlendirilmelidir. Tüm düzenlemeler, kuruluşun kabul edilebilir risk düzeyi ve güvenlik harcamalarının yanı sıra toplanan verilerden etkilenir.

IDC Global Merkezi

5 Speen Street
Framingham, MA 01701
ABD
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Telif Hakkı Bildirimi

IDC Bilgi ve Verilerinin Harici Yayını — Reklamcılık, basın bültenleri veya tanıtım malzemelerinde kullanılacak tüm IDC bilgileri, IDC Başkan Yardımcısının veya Ülke Müdürünün ön yazılı onayını gerektirir. Bu tür bir taleple birlikte önerilen belgenin bir taslağı sunulmalıdır. IDC, herhangi bir nedenle harici kullanım onayını reddetme hakkını saklı tutar.

Copyright 2015 IDC. Yazılı onay olmaksızın çoğaltılması tamamen yasaktır.

IDC Hakkında

International Data Corporation (IDC), pazar istihbaratı, danışmanlık hizmetleri, bilgi teknolojisi etkinlikleri, telekomünikasyon ve tüketici teknolojisi pazarının en önde gelen global sağlayıcısıdır. IDC, BT profesyonellerinin, işletme yöneticilerinin ve yatırım topluluğunun teknoloji alımları ve iş stratejisi ile ilgili gerçeğe dayalı kararlar vermelerine yardımcı olur. 1.100'den fazla IDC analisti, dünya çapında 110'dan fazla ülkede teknoloji, endüstri fırsatları ve eğilimleri konularında global, bölgesel ve yerel uzmanlık sunmaktadır. IDC, 50 yıldır müşterilerinin temel iş hedeflerine ulaşmalarına yardımcı olmak için stratejik bilgiler sağlamaktadır. IDC, dünyanın önde gelen teknoloji ortamı, araştırma ve etkinlik şirketi olan IDG'nin bağlı kuruluşudur.