Teknik broşür

Ağ ve veri güvenliği için uyumluluk şartlarını karşılayın

Baskı filosu üzerinde güvenlik denetimleri uygulamak için öneriler

İçindekiler

Uyumluluk ihlali şirketinize zarar verebilir

Bir güvenlik ihlali, yüksek ceza tutarlarına ve davalara ek olarak gelir kaybına ve itibarınızın zedelenmesine yol açabilir. Güvenlik planınızı oluştururken, ağınızın ancak en zayıf halkanız kadar güvenli olduğunu unutmayın. Bilgisayarların sahip olduğu güvenlik zaaflarının çoğu, baskı ve görüntüleme aygıtları için de geçerlidir. Uyumluluk şartlarını karşılamanıza ve ticari bilgilerinizi güvenlik tehditlerinden korumanıza yardımcı olacak aygıtları ve çözümleri kullanmanız hayati önem taşır.

Risk nedir?

Düzenleme ve yasalara uyum göstermemek, global ölçekteki kuruluşlar için cezalar, iş kaybı, itibar kaybı ve toplu davalar gibi ağır bedellere yol açabilir.

Korunmayan veya yeterli korumaya sahip olmayan uç noktalar siber suçlar için daha fazla fırsat demektir. Ponemon tarafından kısa süre önce yapılan bir çalışma kapsamında düzenlenen ankete katılan kuruluşlar 2016 yılında bir önceki yılın aynı dönemine göre %20 artışla haftada ortalama iki saldırıyla karşı karşıya kalmıştır ve siber suçlara karşı yürütülen mücadelede yıllık 9,5 milyon $ kayba uğramıştır[1]. Yalnızca geçen yıl, dünya genelinde önceki iki yıla göre %400 artışla 4 milyardan fazla veri kaydı ihlal edilmiştir[2].

Pek çok BT departmanı bilgisayarları ve ağı korumak için sıkı güvenlik tedbirlerini hayata geçirse de, baskı ve görüntüleme aygıtları genellikle göz ardı ediliyor. Ancak yazıcılar, ağınıza giriş noktası işlevi görebilir ve güvenli hale getirilmeleri oldukça önemlidir. BT yöneticileri tarafından bildirilen tüm veri ihlallerinin %26'sı yazıcıları içermektedir[3].

Büyüyen bu tehdide karşı koymak için hükümet organları dünya genelinde yeni katı düzenlemeler uygulayarak kuruluşların müşteri bilgilerini daha iyi korumalarını şart koşuyor. Örneğin yeni AB Genel Veri Koruma Yönetmeliği (GDPR) 2018 yılında yürürlüğe girecek olan önemli bir düzenlemedir. GDPR uyarınca, işletmelere verilerin korunması yönünde uygulanan zorunluluklar artacaktır. Bu nedenle, bilgisayarlardan yazıcı ve mobil aygıtlara kadar ağınızdaki tüm aygıtların korunduğundan emin olmanızı tavsiye ederiz. Yeni düzenlemeden yalnızca AB ülkeleri etkilenmemekte, AB'de ikamet edenlerden veri toplayıp bu verileri kullanan tüm global işletmeler de bu yönetmeliğe uymak zorundadır. Güvenlik ihlallerinin tespit edilmesi ve bir ihlal fark edildikten sonra 72 saat içinde bildirilmesi için her bir aygıtın kuruluşlar tarafından izlenip değerlendirilmesi gerekecektir. Uyum denetimleri sırasında ihlallerin takip edilmediği ya da bildirilmediği ortaya çıkarsa işletmelerin 20 milyon €'ya ya da şirketin yıllık cirosunun %4'üne varan para cezası ödemesi söz konusu olacaktır.

Uyumluluğu iyileştirmek için yaygın güvenlik denetimlerini kullanın

Sektördeki uyumluluk şartlarına ve düzenlemelerine ayak uydurmak zorlu bir görev. Neyse ki İnternet Güvenliği Merkezi (CIS), siber güvenlik önerilerini basitleştirmek için bir dizi yaygın güvenlik denetimi oluşturdu. CIS Kritik Güvenlik Denetimleri, siber saldırıları durdurmaya yardımcı olabilecek 20 spesifik eylemi içermektedir. (Ayrıntılar için https://www.cisecurity.org/critical-controls.cfm adresini ziyaret edin.) Denetimler, sektörle ilgili PCI-DSS, ISO 27001, US CERT önerileri, HIPAA, FFIEC ve NIST gibi pek çok diğer düzenlemeyle paralellik içerisindedir. Denetimler bu çerçevelerin yerini almayı amaçlamaz ancak bu çerçeveleri anlamlandırmak için şirketler tarafından sıklıkla kullanılırlar.

CIS Kritik Güvenlik Denetimleri, getirisi yüksek az sayıda eyleme öncelik verir. Belli başlı tehdit raporlarından elde edilen en yaygın saldırı kalıplarına yanıt üretirler. Oluşturulmalarında, aralarında önde gelen adli tıp uzmanlarının ve olaylara yanıt üretmekte uzmanlaşmış kuruluşların da yer aldığı, sektör uzmanlarından oluşan geniş bir grup rol almıştır. Ayrıca, Denetimler gelişen tehditler ve saldırılar temelinde sürekli olarak güncellenmektedir.

Kendi güvenlik eylem planınızı oluşturmak ve uyumluluk düzenlemelerini karşılamak için CIS Kritik Güvenlik Denetimleri'nden yararlanın. Bu broşür, genel güvenlik planınızın bir parçası olarak baskı aygıtlarınızı, verilerinizi ve belgelerinizi güvenceye almanıza yardımcı olmak için, 20 Denetim'in her birine ilişkin eylem önerileri sunmaktadır. 4, 6, 8, 12, 13 ve 15 sayılı denetimler özellikle yeni GDPR şartlarıyla ilişkili veri koruma ve takip faaliyetlerini ele almaktadır.

CIS Kritik Güvenlik Denetimleri ve önerilen eylemler

CSC 1: Yetkilendirilmiş ve Yetkilendirilmemiş Aygıt Envanteri

Denetim – Yalnızca yetkilendirilmiş aygıtlara erişim izni vermek, yetkilendirilmemiş ve yönetilmeyen aygıtları bulup erişimlerini engellemek için tüm donanım aygıtlarınızı etkin bir biçimde yönetin (envanterini alın, izleyin ve düzeltin).

Öneri – Ağınızdaki tüm baskı aygıtlarının hesaba katıldığından ve güvenlik politikanıza uyumlu olacak şekilde etkin bir biçimde yönetildiğinden emin olun. Etkili bir baskı güvenliği yönetim aracı, ağa ve bilgisayarlara bağlı tüm aygıtları keşfedebilir ve bu aygıtların görünür hale gelmelerini sağlar.

CSC 2: Yetkilendirilmiş ve Yetkilendirilmemiş Yazılım Envanteri

Denetim – Yalnızca yetkilendirilmiş yazılımların kurulup çalıştırılmasını sağlamak, yetkilendirilmemiş ve yönetilmeyen yazılımları bulup kurulmalarını veya çalıştırılmalarını engellemek için, ağınızdaki tüm yazılımları etkin bir biçimde yönetin (envanterini alın, izleyin ve düzeltin).

Öneri – Baskı ve görüntüleme aygıtlarınıza yüklenen tüm ürün yazılımlarının ve çözümlerin güncel, orijinal oldukları doğrulanmış ve imzalanmış olduklarından emin olun. Yalnızca orijinal kodların yüklendiğinden emin olmak için, yerleşik BIOS ve ürün yazılımı koruması bulunan baskı aygıtlarını tercih edin. Baskı filosu yönetim çözümleri sayesinde, tüm filo genelinde proaktif ürün yazılımı güncellemeleri yapılması sağlanabilir. Yazılımlar (sunucu ve istemci tabanlı), imzalanmış ve orijinallikleri doğrulanmış olmalıdır.

CSC 3: Mobil Aygıtlarda, Dizüstü Bilgisayarlarda, İş İstasyonlarında ve Sunucularda Güvenli Donanım ve Yazılım Yapılandırmaları

Denetim – Saldırganların tehlikelere açık hizmetleri ve ayarları kullanmalarını önlemek için, sıkı bir yapılandırma yönetimi ve değişiklik denetimi sürecini hayata geçirerek, dizüstü bilgisayarlar, sunucular ve iş istasyonları üzerinde güvenlik yapılandırmaları belirleyin, uygulayın ve etkin bir biçimde yönetin (izleyin, raporlar oluşturun ve düzeltin).

Öneri – Diğer tüm ağ uç noktaları gibi yazıcılar da güvenli olacak şekilde yapılandırılmalıdır. Tüm baskı aygıtlarınızı kapsayacak bir güvenlik politikası oluşturup uygulamanız ve bu politikaya aykırılık teşkil eden durumları etkin bir biçimde düzeltmeniz gerekir. Güvenlik kontrol listeleri (ör. NIST) veya güvenlik danışmanlığı hizmetleri, kapsamlı bir güvenlik politikası tasarlayıp uygulamanıza yardımcı olabilir. Etkili bir baskı güvenliği yönetim aracı, baskı filonuz genelinde politika oluşturma, aygıt ayarlarını uygulama, değerlendirme ve düzeltme süreçlerini otomatik hale getirebilir. Kurumsal düzeydeki çok işlevli yazıcılarda (MFP'ler) 250'den fazla güvenlik ayarı bulunduğundan, bu süreci otomatik hale getirmek size büyük bir zaman tasarrufu sağlayacaktır.

CSC 4: Sürekli Zayıf Nokta Değerlendirmesi ve Düzeltme

Denetim – Zayıf noktaları belirlemek, düzeltmek ve saldırganlar için fırsat penceresini olabildiğince daraltmak için sürekli olarak yeni bilgiler edinin, bu bilgileri değerlendirin ve gerekli adımları atın.

Öneri – ArcSight, Splunk veya SIEMonster gibi Güvenlik Bilgileri ve Olay Yönetimi (SIEM) çözümleri, ağınızdaki hareketliliği gerçek zamanlı olarak izleyebilir ve olaylar meydana geldiğinde yöneticileri bilgilendirebilir. Yazıcıları izlemek, bilgisayarları izlemek kadar önemlidir. Yazıcılarınızın SIEM aracına olay syslog mesajları gönderebildiğinden emin olun.

Çalışma sürelerini en yüksek düzeye çıkarıp BT müdahalelerini en az indirmek için, saldırıları gerçek zamanlı izleme ve otomatik olarak kurtarma özelliklerine sahip baskı aygıtlarını tercih edin.

Zayıf noktaları en aza indirmek için, yeni yazıcıları ağa bağlandıkları anda belirleyip kurumsal güvenlik politikanızı onlara otomatik olarak uygulayabilen bir filo güvenliği yönetim aracı kullanın. Tüm baskı filonuzun politikanıza uygunluğunu korumak için, düzenli değerlendirmeler/düzeltmeler planlayın.

CSC 5: Yönetici Ayrıcalıklarının Denetimli Kullanımı

Denetim – Bilgisayarlar, ağlar ve uygulamalar üzerindeki yönetici ayrıcalıkları kullanımlarını, atamalarını ve yapılandırmalarını izleyin, denetleyin, önleyin ve düzeltin.

Öneri – Aygıt ayarlarını yalnızca BT personelinin veya yetkili diğer kişilerin kurup yapılandırdığından emin olmak için, kullanıcıları doğrulama ve işlevlere erişimi kişilerin rollerine göre denetleme becerilerine sahip baskı aygıtlarını ve çözümlerini tercih edin. Filo genelinde yönetici şifrelerinin kullanılmasını sağlamak için filo güvenliği yönetim yazılımı kullanın.

CSC 6: Denetim Kayıtlarının Tutulması, İzlenmesi ve Analiz Edilmesi

Denetim – Bir saldırıyı belirlemenize, anlamanıza veya ondan kurtulmanıza yardımcı olabilecek olay denetim kayıtlarını bir araya getirin, yönetin ve analiz edin.

Öneri – Baskı aygıtlarının olay syslog mesajları oluşturabilmesi gerekir. Bu sayede güvenlik ekibiniz sorunları keşfetmek ve çözmek için denetim kayıtlarını düzenli olarak inceleyebilir. Bu mesajları filo güvenliği yönetim çözümlerine ve SIEM araçlarına, hem gerçek zamanlı izleme hem de denetimler veya diğer uyumluluk şartları için raporlar oluşturma amaçları için gönderebilme özelliğine sahip aygıtları tercih edin.

CSC 7: E-posta ve Web Tarayıcısı Korumaları

Denetim – Saldırı yüzeyini ve saldırganların web tarayıcıları ve e-posta sistemleri üzerinden insan davranışlarını manipüle etme fırsatlarını en aza indirin.

Öneri – MFP'ler genellikle internete bağlı olduklarından, örneğin taranmış belgeleri e-posta ile gönderebilirler. E-posta ile gönderilen taranmış belgelerin hassas verilerin korunmasını sağlayacak şekilde şifrelendiklerinden emin olun. Kullanıcıları doğrulama ve aygıt içerisindeki kaynaklara erişimi (örneğin web sunucularına veya e-posta işlevine) kişilerin rollerine bağlı olarak denetleme becerilerine sahip aygıtları ve çözümleri kullanın. MFP'leriniz için "Güvenilir Siteler" listesi oluşturun ve aygıttan yalnızca güvenilir web sitelerine erişilebilmesini sağlamak için bu listeyi gerektiği gibi yönetin. Düzenli hale getirilmiş yönetim ve artırılmış güvenlik için çeşitli kimlik doğrulama yöntemlerini (örneğin PIN/PIC, LDAP veya Kerberos kimlik doğrulaması) Active Directory ile bütünleştirin. Ağa bağlı baskı aygıtlarında yerleşik kötü amaçlı yazılım ve virüs koruması bulunmalı, en güncel korumaların geçerli olması için yazıcı yazılımları düzenli olarak güncellenmelidir.

CSC 8: Kötü Amaçlı Yazılımlara Karşı Korumalar

Denetim – Bir yandan kötü amaçlı kodların şirketiniz içerisindeki farklı noktalarda kurulmalarını, yayılmalarını ve çalıştırılmalarını denetlerken diğer yandan savunma, veri toplama ve düzeltici eylem önlemlerinin hızla güncellenebilmesi için otomatik yöntemlerin kullanımını optimize edin.

Öneri – Yalnızca doğrulanmış ve imzalanmış kodları yükleyen, aygıt belleğini izlemek ve saldırı durumunda aygıtı yeniden başlatmak için yerleşik kötü amaçlı yazılım önleme özelliklerine sahip baskı aygıtlarını tercih edin. Etkili bir baskı güvenliği yönetim aracı, filo genelinde aygıt ayarlarını otomatik olarak değerlendirip düzeltebilir. Ayrıca, tüm baskı yazılımı çözümlerinin imzalanmış ve orijinalliği doğrulanmış olduğundan emin olun.

CSC 9: Ağ Bağlantı Noktalarının, Protokollerinin ve Hizmetlerinin Sınırlandırılması

Denetim – Saldırganlara açık zayıf noktaları en aza indirmek için, ağa bağlı aygıtlar üzerindeki bağlantı noktalarının, protokollerin ve hizmetlerin süregelen işletimsel kullanımını yönetin (izleyin, denetleyin ve düzeltin).

Öneri – Varsayılan olarak devre dışı bırakılmamış olmaları durumunda, saldırganların aygıta erişmek için yararlanabilecekleri kullanılmayan bağlantı noktalarını ve güvenli olmayan protokolleri (örneğin FTP veya Telnet) devre dışı bırakın. Filo genelinde aygıt ayarlarını otomatik olarak uyumlu tutmak için bir baskı güvenliği yönetim aracı kullanarak BT departmanının zamandan tasarruf etmesini sağlayın ve riskleri azaltın. Aygıt işlevlerine ve ayarlarına erişimi sınırlandırmak için yönetici şifreleri, kimlik doğrulama ve rol esaslı erişim denetimleri kullanın.

CSC 10: Veri Kurtarma Özelliği

Denetim – Verileri zamanında kurtarabilmek için, kanıtlanmış bir metodoloji kullanarak kritik bilgileri düzgün şekilde yedekleyin.

Öneri – Bu Denetim halihazırda yazıcılar için geçerli değildir.

CSC 11: Ağ Aygıtları için, Güvenlik Duvarları, Yönlendiriciler ve Anahtarlar gibi Güvenli Yapılandırmalar

Denetim – Saldırganların tehlikelere açık hizmetleri ve ayarları kullanmalarını önlemek için, sıkı bir yapılandırma yönetimi ve değişiklik denetimi sürecini hayata geçirerek, ağ altyapısı aygıtları üzerinde güvenlik yapılandırması belirleyin, uygulayın ve etkin bir biçimde yönetin (izleyin, raporlar oluşturun ve düzeltin).

Öneri – Yazıcılar da ağda yer alır ve diğer tüm ağ uç noktaları gibi güvenli olacak şekilde yapılandırılmaları gerekir. Etkili bir baskı güvenliği yönetim aracı, ağı güvende tutarken BT departmanına zaman tasarrufu sağlamak için filo genelinde aygıt ayarlarını uygulama, değerlendirme ve düzeltme süreçlerini otomatik hale getirebilir.

CSC 12: Sınır Koruması

Denetim – Güvenliğe zarar verici verilere odaklanarak, farklı güven düzeylerine sahip bilgi aktarım ağlarındaki akış üzerinde tespit, önleme ve düzeltme eylemleri gerçekleştirin.

Öneri – Aktarım halindeki (yazıcıya veya yazıcıdan giden baskı ya da tarama görevleri) veya aygıtın sabit sürücüsünde bulunan verileri korumak için şifreleme kullanın. Kullanıcı kimliği doğrulama ve örneğin, yalnızca yetkilendirilmiş kullanıcıların taranmış belgeleri e-posta ile gönderebilmelerini veya dosyaları bulut hedeflerine yönlendirebilmelerini sağlama gibi, belirli bir işleve erişimi kişilerin rollerine bağlı olarak denetleyebilme özelliklerine sahip baskı aygıtlarını ve çözümlerini tercih edin. Kötü amaçlı web sitelerine erişimi engellemek için aygıt üzerindeki "Güvenilir Siteler" listesinde güvenilir web sitelerini yapılandırın. Güvenli mobil baskı çözümleri bir yandan ağı korurken diğer yandan kullanıcıların mobil aygıtlarından baskı almalarını kolaylaştırabilir.

CSC 13: Veri Koruması

Denetim – Verilerin dışarı sızmasını önleyin, dışarı sızmış verilerin yarattığı etkileri azaltın ve hassas bilgilerin gizliliğini ve sağlamlığını koruyun.

Öneri – Aktarım halindeki (yazıcıya veya yazıcıdan giden baskı ya da tarama görevleri) veya aygıtın sabit sürücüsünde bulunan verileri korumak için şifreleme kullanın. Hassas belgelerin çıkış tepsilerinde bırakılmasını önlemek için kimlik doğrulamalı baskı çözümlerini kullanın. Kiralanmış aygıtları iade etmeden veya kullanım ömrü tamamlanmış aygıtları geri dönüşüme göndermeden önce aygıtların sabit sürücülerinde kayıtlı verilerin güvenli bir biçimde silindiğinden emin olun.

CSC 14: Bilmesi Gerekenlerle Sınırlı Erişim Denetimi

Denetim – Onaylanmış bir sınıflandırma temelinde, hangi kişilerin, bilgisayarların ve uygulamaların kritik varlıklara (ör. bilgiler, kaynaklar ve sistemler) erişmesi gerektiğini resmi olarak belirleyerek bu kritik varlıklara erişimi izleyin, denetleyin, önleyin, düzeltin ve güvenli hale getirin.

Öneri – Kullanıcıları doğrulama ve işlevlere erişimi kişilerin rollerine bağlı olarak denetleme becerilerine sahip baskı aygıtlarını ve çözümlerini tercih edin. Düzenli hale getirilmiş yönetim ve artırılmış güvenlik için çeşitli kimlik doğrulama yöntemlerini (örneğin PIN/PIC, LDAP veya Kerberos kimlik doğrulaması) Active Directory ile bütünleştirin. Kimlik doğrulamalı baskı çözümleri hassas belgelerin yanlış ellere geçmesini önleyebilir.

CSC 15: Kablosuz Erişim Denetimi

Denetim – Kablosuz yerel alan ağlarının (LAN'lar), erişim noktalarının ve kablosuz istemci sistemlerinin güvenlik kullanımını izleyin, denetleyin, önleyin ve düzeltin.

Öneri – Etkili bir baskı güvenliği yönetim aracı, filo genelinde, kablosuz ayarları da dahil olmak üzere aygıt ayarlarını uygulama, değerlendirme ve düzeltme süreçlerini otomatik hale getirebilir. Taranmış belgeleri e-posta ile gönderme gibi aygıt işlevlerine erişimi kullanıcıların rollerine bağlı olarak sınırlandırmak için erişim denetimi çözümleri kullanın. Güvenli mobil baskı çözümleri bir yandan ağı korurken diğer yandan kullanıcıların mobil aygıtlarından baskı almalarını kolaylaştırabilir. Örneğin, eşler arası kablosuz baskıyı destekleyen aygıtlar, mobil aygıt kullanıcılarının şirketin ağına veya kablosuz hizmetine giriş yapmadan, doğrudan yazıcının kendine has kablosuz sinyaline bağlanarak baskı alabilir.

CSC 16: Hesapların İzlenmesi ve Denetimi

Denetim – Saldırganların müdahale şanslarını en aza indirmek için, sistem ve uygulama hesaplarının yaşam döngülerini -oluşturulma, kullanım, askıda kalma ve silinme durumlarını- etkin bir biçimde yönetin.

Öneri – Kullanıcıları doğrulama ve işlevlere erişimi kişilerin rollerine göre denetleme becerilerine sahip baskı aygıtlarını ve çözümlerini tercih edin. Merkezileştirilmiş yönetim ve artırılmış güvenlik için, kimlik doğrulamayı Active Directory ile bütünleştirin. Kullanıcı hesaplarını düzenli olarak gözden geçirin ve gerekli olmayanları devre dışı bırakın; hesap kullanımını takip etmek için izleme çözümlerinden yararlanın. Hesap kullanıcı adlarını ve kimlik doğrulama bilgilerini, hem aktarım halinde hem de aygıt belleğinde saklandıkları süre boyunca şifreleyin. Güvenlik danışmanları, riskleri en aza indirmenize yardımcı olmak için kapsamlı bir baskı güvenliği planı tasarlamanıza ve bazı durumlarda hesapları izleme ve denetleme de dahil olmak üzere güvenliği yönetmenize yardımcı olabilirler.

CSC 17: Güvenlik Becerileri Değerlendirmesi ve Boşlukları Doldurmak için Uygun Eğitimler

Denetim – Şirketin korunmasına katkı sunmak için gerekli olan spesifik bilgileri, becerileri ve vasıfları tespit edin; kuruluştaki tüm işlevsel roller için politika, kurumsal planlama, eğitim ve farkındalık programları aracılığıyla boşlukları değerlendirmek, belirlemek ve doldurmak için bütünsel bir plan geliştirin ve uygulayın.

Öneri – Baskı güvenliği danışmanları güvenlik risklerinizi değerlendirmenize, kapsamlı bir güvenlik politikası ve planı geliştirmenize ve süreç ve teknoloji önerilerini hayata geçirmenize yardımcı olacak profesyonel bilgilere sahiptirler. Hatta bazı güvenlik hizmetleri, baskı güvenliği ve uyumluluğunu sizin adınıza yönetebilir.

CSC 18: Uygulama Yazılımı Güvenliği

Denetim – Güvenlik zafiyetini önlemek, belirlemek ve düzeltmek için, kendi geliştirdiğiniz ve dışarıdan aldığınız yazılımların güvenlik yaşam döngülerini yönetin.

Öneri – Geliştirilmiş tüm baskı çözümleriyle ilgili olarak güvenli geliştirme en iyi uygulamalarına bağlı kalın. İmzalanmış ve orijinal olduğu doğrulanmış yazılım çözümlerini tercih edin.

CSC 19: Olaylara Yanıt ve Yönetim

Denetim – Olaylara yanıt altyapısı (ör. planlar, tanımlanmış roller, eğitim, iletişimler ve yönetim izlemesi) geliştirip uygulayarak şirket bilgilerini ve itibarını koruyun.

Öneri – Olaylara yanıt planınızın baskı ortamınızı da içerdiğinden emin olun.

CSC 20: Nüfuz Testleri ve Kırmızı Takım Alıştırmaları

Denetim – Saldırganın amaçlarını ve eylemlerini taklit ederek, şirketin savunma bileşenlerinin (teknoloji, süreçler ve insanlar) toplam kuvvetini test edin.

Öneri – Nüfuz testlerine baskı ortamınızı da dahil edin. Zayıf noktalara karşı baskı ortamınızı düzenli olarak değerlendirin ve bu zafiyetleri gidermek için güvenlik planınızı güncelleyin.

Bir sonraki adıma geçin

Bu teknik broşürde yer alan önerileri hayata geçirmeniz baskı güvenliğinizi sıkılaştırmanıza ve uyumluluk şartlarını karşılamanıza yardımcı olabilir. Desteğe mi ihtiyacınız var? Baskı güvenliği yönetim ve danışmanlık hizmetleri, baskı aygıtlarınızın, verilerinizin ve belgelerinizin güvenliğini artırmak için bir plan geliştirmenize ve gerekli süreçleri ve teknolojiyi uygulamaya koymanıza yardımcı olabilir.

Ek A: HP baskı güvenliği özellikleri, çözümleri ve hizmetleri

HP aygıtlarında yerleşik olarak bulunan güvenlik özellikleri ve sektörde öncü yazılım çözümleri ve hizmetleri, uyumluluk şartlarını içeren yasalara ve düzenlemelere uygunluk sağlamanıza ve ticari bilgilerinizi güvenlik tehditlerinden korumanıza yardımcı olabilir.

Yerleşik güvenlik özellikleri HP Enterprise sınıfı yazıcılarınızı ve MFP'lerinizi kötü amaçlı yazılımlara karşı korur ve saldırıları otomatik olarak belirleyip kurtarma işlemlerini gerçekleştirir. Yalnızca HP, baskı güvenliği, tehditleri ortaya çıktıkları anda durduracak gerçek zamanlı tespit, otomatikleştirilmiş izleme ve yerleşik yazılım doğrulaması özellikleri sunar[4]. (CSC'nin 2., 4., 6. ve 8. maddelerini karşılamanıza yardımcı olur.) hp.com/go/PrintersThatProtect

HP Access Control çözümleri, olası güvenlik ihlallerini azaltmanıza yardımcı olmak ve iş muhasebesi ve izleme için çeşitli kimlik doğrulama ve rol esaslı erişim denetimleri sunar. (CSC'nin 5., 7., 10., 12., 13., 14., 15. ve 16. maddelerini karşılamanıza yardımcı olur.) hp.com/go/hpac

Şifreleme ve **HP JetAdvantage İş Akışı Çözümleri**, verileri hem HP Enterprise aygıtlarında depolandıkları süre boyunca hem de baskı aygıtlarına veya buluta gidiş-gelişleri sırasında korur. (CSC'nin 12. ve 13. maddelerini karşılamanıza yardımcı olur.) hp.com/go/upd, hp.com/go/documentmanagement

HP kimlik doğrulamalı baskı çözümleri, baskı işlerinizi korumalı bir sunucuda, bulutta veya bilgisayarınızda saklayarak korur. Kullanıcılar, baskı işlerini seçtikleri noktada çekip basabilmeleri için kimlik doğrulamasına tabi tutulur. (CSC'nin 10., 13. ve 14. maddelerini karşılamanıza yardımcı olur.) hp.com/go/hpac, hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Connect, güvenliği koruyup ihtiyaç duyduğunuz yönetimsel kontrolü sağlarken, aynı zamanda kullanıcıların akıllı telefonlarından veya tabletlerinden kolayca baskı alabilmelerini sağlar. (CSC'nin 12. ve 15. maddelerini karşılamanıza yardımcı olur.) hp.com/go/JetAdvantageConnect

HP yazıcı olay verileri, ArcSight, Splunk veya SIEMonster gibi SIEM araçlarına gönderilebilir. Güvenlik ekibiniz, genel BT ekosisteminin bir parçası olarak yazıcı uç noktalarını kolayca görebilir ve düzeltici eylemleri uygulamaya koyabilir. (CSC'nin 4. ve 6. maddelerini karşılamanıza yardımcı olur.)

HP JetAdvantage Security Manager, sektörde politika esaslı tek güvenlik uyumluluğu aracıdır[5]. Tüm filoyu kapsayan bir güvenlik politikası belirlemenize, aygıt ayarlarını düzeltme işlemlerini otomatik hale getirmenize, benzersiz sertifikalar yükleyip yenilemenize ve uyumluluğu kanıtlamak için gerekli raporları almanıza yardımcı olur. Çözümün içerdiği Anında Açılma özelliği, ağa eklendiklerinde veya bir yeniden başlatma sonrasında yeni aygıtları otomatik olarak yapılandırır. (CSC'nin 1., 2., 3., 4., 5., 6., 8., 9., 11. ve 15. maddelerini karşılamanıza yardımcı olur.) hp.com/go/securitymanager

HP Güvenli Yönetilen Baskı Hizmetleri, sektördeki en güçlü, en kapsamlı baskı güvenliği korumalarını sunar[6]. Baskı güvenliği karmaşık olabilir. Aygıt güvenliğini sıkılaştırmaktan kişilere, süreçlere ve uyumluluk şartlarına yönelik gelişmiş güvenlik çözümlerine kadar, baskı güvenliğinizi yönetme işini HP'ye bırakın. (CSC'nin 2., 3., 12., 16., 17., 18 ve 19. maddelerini karşılamanıza yardımcı olur.) hp.com/go/SecureMPS

HP Baskı Güvenliği Profesyonel Hizmetleri, baskı ortamınızı değerlendirme, proaktif bir biçimde güvenlik politikaları belirleme ve güvenlik planınızı güncel tutma konusunda güvenlik uzmanlarından destek almanızı sağlar. Hatta baskı güvenliği uyumluluğunuzu sizin adınıza yönetebiliriz. (CSC'nin 2., 3., 12., 16., 17. ve 19. maddelerini karşılamanıza yardımcı olur.) hp.com/go/SecureMPS

Notlar

[1] HPE sponsorluğunda gerçekleştirilen Ponemon Çalışması "2016 Cost of Cyber Crime Study & the Risk of Business Innovation" (2016 Yılı Siber Suçların Maliyeti Çalışması ve Ticari Yeniliğin Riskleri), 2016.

[2] RiskBased Security tarafından düzenlenen 2016 Year End Data Breach QuickView (2016 Yıl Sonu Veri İhlallerine Hızlı Bakış) başlıklı rapor, Ocak 2017.

[3] Anket katılımcılarının %26,2'si, onarım gerektiren ciddi bir BT güvenlik ihlaliyle karşılaşmıştır ve bu olayların %26,1'inden fazlası baskı işlemlerini içermektedir. IDC, "IT and Print Security Survey 2015" IDC #US40612015, Eylül 2015.

[4] 2015'ten itibaren sunulan HP Enterprise sınıfı aygıtlar için geçerlidir ve HP'nin 2016 yılında, aynı sınıftaki rakip yazıcıların yayınlanmış yerleşik güvenlik özellikleri üzerinde yaptığı incelemeyi baz almaktadır. Yalnızca HP, bütünlük kontrollerinden kendi kendini onarma becerisine sahip BIOS'a kadar uzanan güvenlik özelliklerinin bir bileşimini sunar. Güvenlik özelliklerini etkinleştirmek için FutureSmart hizmet paketinin güncellenmesi gerekebilir. Uyumlu ürünlerin listesini görmek için hp.com/go/PrintersThatProtect adresini ziyaret edin. Daha fazla bilgi için hp.com/go/printersecurityclaims adresini ziyaret edin.

[5] HP JetAdvantage Security Manager ayrıca satın alınmalıdır. Daha fazla bilgi edinmek için lütfen hp.com/go/securitymanager adresini ziyaret edin. Rekabetçilik iddiası, rakip teklifleri (Aygıt Güvenliği Karşılaştırması, Ocak 2015) ve Buyers Laboratory LLC tarafından, Şubat 2015'te sunulan, HP JetAdvantage Security Manager 2.1 ile ilgili Çözümler Raporu üzerinde gerçekleştirilen HP kurum içi araştırmalarını baz almaktadır.

[6] Önde gelen yönetilen baskı hizmeti sağlayıcıları tarafından sunulan aygıt, veri ve belge güvenliği özellikleri içerir. HP'nin, 2015-2016 yıllarında, aynı sınıftaki rakip yazıcılara ilişkin güvenlik hizmetleri, güvenlik ve yönetim yazılımları ve aygıtlarda yerleşik güvenlik özelikleriyle ilgili olarak kamuoyuna açıklanmış bilgiler üzerinde gerçekleştirdiği incelemeyi baz almaktadır. Daha fazla bilgi için hp.com/go/MPSsecurityclaims veya hp.com/go/mps adreslerini ziyaret edin.

Güncellemeler için üye olun
hp.com/go/getupdated

İş arkadaşlarınızla paylaşın

4AA6-8821TRE, Haziran 2017, Rev. 1