****

**Siber Olaylara Müdahale (SOME) Birimi**

**Çok Fonksiyonlu Yazıcılarda (MFP) Alınması Gereken Güvenlik Önlemleri Dökümanı v.1.0**

**HAZIRLAYAN**

Cihan Mehmet DOĞAN

(Sızma Testi Uzmanı)

**28.10.2019**

**ÖZET**

Bir yazıcının seri ya da paralel olarak doğrudan bağlandığı ve bilgisayarla direk haberleştiği sistemler eskide kalmıştır. Kopyalama, yazdırma, tarama ve fax çekme özelliğine sahip ayrı ayrı cihazlar tek bir cihaz halini aldılar. Bu yapıdaki cihazlar MDF (Multifuntional Devices) ismiyle anılmaya başladılar. Günümüz teknolojileriyle gelişen dünyada artık yazıcılarda doğrudan networke bağlanarak uzaktan yönetilebilir hale evrildiler. Bu değişimlerle beraber her ağ cihazında olduğu gibi multifonksiyonel yazıcı cihazlarında da güvenlik zafiyetleri ve eksik cihaz yapılandırmaları tehdit etmektedir. Ağda bulunan cihazlara oranla IoT, yazıcı ve multifonksiyonel cihazlar kendilerine has iletişim protokolleri gereği daha kolay istismar edilebilmektedir.



Bu dökümanda yazıcı cihazların sıkılaştırılmasıyla ilgili adımlar yer almaktadır. İlgili sistemlerde kullanılan yazıcı cihazlarının sıkılaştırmalarının yapılması gerekmektedir. İlgili sistemlere yapılabilecek siber saldırılar yalnızca yerel network(ağ) üzerinden gelmeyebilir. İlgili sistemlere iç ağlardan gelecek erişimler ve kullanıcı bazlı erişimler de dikkate alınarak gerekli sıkılaştırmaların (güvenlik ayarları, güncellemeler, ağ katmanında erişim kısıtlaması, kullanıcı fonksiyon kısıtlaması vb.) yapılması büyük önem taşımaktadır.

**Genel Kontrol Prosedürleri**

1. **Girişler için Genel Güvenlik Prosedürleri**
2. **Yazıcı için Güvenli Bir Yönetici Parolasını Belirleme**

İlk kez kurulan yazıcıların varsayılan olarak gelen yazıcı yönetici parolalarının değiştirilmesi gerekmektedir. Varsayılan olarak bırakılan parolalar saldırganlar tarafından tahmin edilebileceği için ciddi bir güvenlik zaafiyeti oluşturmaktadır. Bu parolaların değiştirilmesi gerekmektedir. Bu parola bakanlığımızın BGYS Parola Yönetimi Politikası dökümanı 4.2 Parola Politikası başlığına uygun olarak belirlenmesi gerekmektedir.

<https://bilgiguvenligi.saglik.gov.tr/files/BGYS_Dokuman_Ornekleri/BG.PO...%20PAROLA%20Y%C3%96NET%C4%B0M%C4%B0%20POL%C4%B0T%C4%B0KASI.pdf>

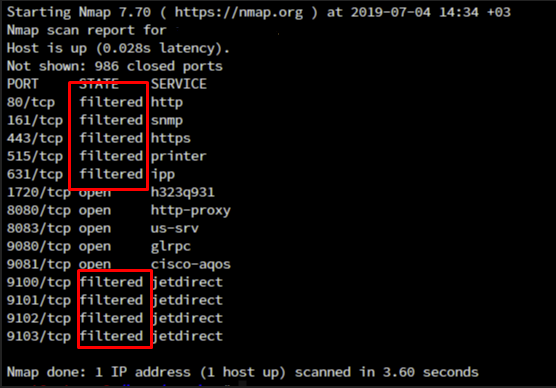
1. **Yazıcı Web Kontrol Arayüzü Yönetici Şifresinin Değiştirilmesi**

Yazıcıların genellikle uzaktan erişilebilmesine imkân sağlayan web yönetim arayüzleri bulunmaktadır. Bu arayüzden yönetici istediği ayar ve değişiklikleri yapabilmektedir. Bu arayüzler genellikle güvenlik kodu (captcha) destekli olmamaktadır. Captcha destekli olmayan bir arayüz kaba kuvvet (brute force) saldırılarına açıktır. Kaba kuvvet saldırısı özet olarak rastgele olarak oluşturulan parolaların bizim parolamız olarak denenmesine dayanır. Üretilen rastgele parola sayısı ve kombinasyonuna göre bu saldırının başarı olasılığı artmaktadır.

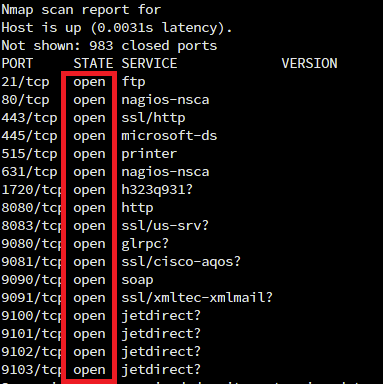
1. **Yazıcı Cihazı Network içinde Güvenlik Duvarının Arkasına Konumlandırma**

Yazıcıyı doğrudan internet ortamına bağlamayın, Güvenlik duvarı, IDS/IPS tarzı bir güvenlik cihazının arkasına konumlandırın. İnternete doğrudan bağlanırsa portların taranma durumu web servisleri gibi belli servislerde zafiyet bulunabileceğini unutmayınız. **Güvenlik duvarı arkasına aldığınız yazıcıların belli yönetim ipleri hariç port erişimlerini sınırlandırın.**

***Firewall arkasına konumlanan bir yazıcıya ait nmap tarama çıktısı***



***Firewall arkasına konumlanmayan bir yazıcıya ait nmap tarama çıktısı***



**B. Network Güvenliği için Genel Güvenlik Prosedürleri**

**Port Listesi**

|  |  |  |  |
| --- | --- | --- | --- |
| **Protokol** | **Port Numarası** | **Ayar** | **Not** |
| **FTP Sunucu** | **TCP 21** | **Riskli** | **Dosya aktarma protokolü** |
| **HTTP** | **TCP 80** | **Riskli** | **Web arayüz servisi** |
| **NetBEUI** | **TCP 139** |  | **Dosya paylaşımı ve yazdırma hizmetleri için ve bir belge almak için veri aktarımında kullanılan küçük bir ağ protokolü** |
| **HTTPS** | **TCP 443** |  | **HTTPS, TLS kullanarak şifreleme gerçekleştiren bir protokoldür.** |
| **IPP over TLS** | **TCP 443** |  | **IPP Internet Printing Protocol olarak bilinmektedir.** **İstemcilerin yazıcıya veya yazdırma sunucusuna bir veya daha fazla yazdırma işi göndermesini ve bir yazıcının durumunu sorgulamak, yazdırma işlerinin durumunu elde etmek veya tek tek yazdırma işlerini iptal etmek gibi görevleri gerçekleştirmesini sağlar. Bu protokolün haberleşmesinin TLS üzerinden yapılması trafiğin manipüle edilmesini engelleyecektir.** |
| **LPD** | **TCP 515** | **Riskli** | **LPD, metin dosyalarını veya Postscriptleri yazdırmak için kullanılan bir yazdırma protokolüdür.** |
| **IPP** | **TCP 631** | **Riskli** | **Internet Printing Protocol** |
| **ThinPrint** | **TCP 4000** |  |  |
| **WSD Scan** | **TCP 5358** |  |  |
| **WSD Print** | **TCP 5358** |  |  |
| **Enhanced WSD** | **TCP 9090** |  |  |
| **Enhanced WSD over TLS** | **TCP 9091** |  |  |
| **RAW** | **TCP 9100-9103** | **Riskli** |  |
| **SNMP v1/v2** | **UDP161** | **Aktif Edilmemeli** |  |
| **SNMP v3** | **UDP161** |  |  |

**Yazıcı Bazlı Portların Teşkil Ettikleri Risk Faktörleri**

**TCP port 80 (HTTP Protokolu Kaynaklı Risk Faktörleri)**

* Yazıcı web arayüzü üzerinden akan veriler (kullanıcı adı, parola vb.) sniff edilerek açık metin olarak elde edilebilir.

**TCP port 23 (Telnet Protokolü Kaynaklı Risk Faktörleri)**

* Telnet işlevi bazen web arabirimine kıyasla sınırlı olsada, ağ, parola ve erişim listesi bilgilerini değiştirmek, ayrıca yazdırma sıralarını izlemek ve yönetmek için de kullanılabilir. Telnet şifrelenmemiş ve güvensiz bir protokol olarak kabul edilir. Kimlik doğrulama ve yapılandırma bilgileri gibi hassas veriler ağdan alınabilecekleri açık bir şekilde gönderilir.

**TCP port 161 (SNMP Protokolü Kaynaklı Risk Faktörleri)**

* SNMP ayar cümlecikleri (benzer olarak parolalarda) genellikle salt okunur erişim için "özel" olarak ayarlanır.
* Saldırgan, yazıcılar hakkında yapılandırma bilgileri toplamak için SNMP kullanabilir veya yapılandırmayı değiştirebilir.
* SNMP, v1 de şifrelenmeyen ağ konfigürasyon dizgeleri ve v2'de ise şifrelenen dizgelerin sözlük saldırısı ile kırılması bilinen zafiyetleridir. Bunların dışında v1 ve v2’nin etkilendiği belli dos atak zafiyetleri bulunmaktadır. Ağdan alınabilen konfigürasyon dizgelerini v3 üzerinden aktarmak güvenli olan bir yöntemdir.
* Cihaz SNMP yazma yeteneğine sahipse, konfigürasyon bilgileri değiştirilebilir.

**TCP Port 9100 (a.k.a. HP JetDirect veya Socket Raw Protokolü Portu Kaynaklı Risk Faktörleri)**

* Yetkisiz uzaktan yazdırma fonksiyonu olduğu için kesinlikle port erişimi firewall kontrollü olmalıdır.
* LCD panelinin değiştirilmesi, karmaşıklığa sebebiyet verecek yazıların yazılması veya kapıyı sosyal mühendislik amaçları için açmak ("Hata oluştu XXX numaralı telefonu arayın."). Bu, 9100 HiJetter portunun istismarı ile yapılabilir.

**TCP port 515 (LPD (Line Printer Daemon) Protokolü Kaynaklı Risk Faktörleri)**

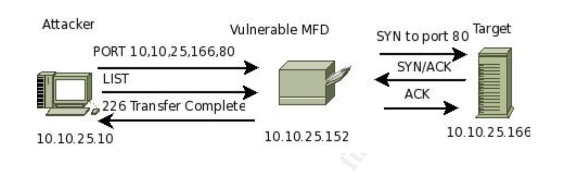
* Yetkisiz uzaktan yazdırma fonksiyonu olduğu için kesinlikle port erişimi firewall kontrollü olmalıdır.
* Trafikte dolaşan veriler açık metin olarak gönderilip alındığı için ağda sniff edilebilir.

**TCP port 631 (IPP The Internet Printing Protokolü Kaynaklı Risk Faktörleri)**

* Yanlış yapılandırılmışsa izinsiz uzaktan yazdırma fonksiyonu bulunmaktadır.
* TLS kullanacak şekilde yapılandırılmadıysa, ağın dinlenebilir (sniff).

**TCP port 21 (FTP Dosya Transfer Protokolü Kaynaklı Risk Faktörleri)**

* FTP kimlik doğrulaması ve aktarımı şifrelenmemiş olduğundan, oturum açma kimlik bilgileri ve verileri ağda sniff edilebilir.
* FTP Bounce atağı FTP server ile diğer bir bilgisayar arasında bağlantı kurmayı amaçlar. Saldırgan kimliğini gizler ve FTP üzerinden erişim yapar. Bugün birçok FTP sunucusunda bu mümkün olmasada, bazı yazıcı modellerinde hala mümkündür.



**TCP port 25 (SMTP Protokolü Kaynaklı Risk Faktörleri)**

* SMTP'nin şifrelenmemiş olması, verilerin ağ üzerinden koklanabileceği anlamına gelir.
* Gelen bir SMTP sunucusu, SMTP rölesi olarak kullanılabilir ve spam gönderilmesine sebebiyet verebilir.

**TCP port 139 (SMB Protokolü Kaynaklı Risk Faktörleri)**

* SMB şifrelenmemiş bir protokoldür. Kimlik doğrulama bilgileri ve veriler ağdan sniff edilebilir.
* SMB servisi üzerinde kimlik doğrulama yapılandırılmadıysa izinsiz yazdırma yapılabilir.

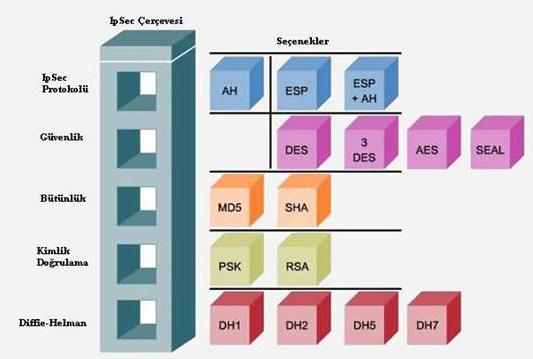
1. **Şifreli İletişim Kanallarının Ayarlanması (SSL/TLS İletişim Protokolleri)**

Ağ içerisinde yazıcı cihazının ağ içerisinde bulunan diğer cihazlarla iletişimi olacaktır. Bu iletişimi SSL / TLS şifreleme protokolleri üzerinden yaparak ağ paketlerinin güvenli bir şekilde ağ içerisinde dolaşımda olmasını sağlayabiliriz. SSL/TLS, IPPS (Internet Printing Protokol) protokolünü yazdırma sırasında veya yazıcıdan e-posta gönderirken kullanılır. TLS versiyonu ve şifreleme algoritması seçimi bu iletimin güvenliği açısından önem arz etmektedir. TLS’in eski versiyonlarında bilinen mevcut zafiyetlerden dolayı TLS’in 1.2 versiyonu ve şifreleme algoritması olarak ise AES kullanılması gerekmektedir. Bu iletişimde cihazın ürettiği sertifika ya da kurum tarafından tahsil edilen SSL sertifikaları kullanılabilir. SSL/TLS aşağıdaki protokollere uygulanmalıdır:

* IPP over SSL
* POP3 over SSL
* SMTP over SSL
* FTP over SSL
* DSM over SSL
* eSCL over SSL
* HTTPS
* LDAP over SSL
* Enhanced WSD over SSL
* REST over SSL

1. **Şifreli İletişim Kanallarının Ayarlanması (IPsec Protokol)**

IPsec iletimi, bilgiyi çeşitli sızıntılar ve veri sahteciliğinden korumak için herhangi bir uygulama yazılımı veya ağ mimarisine güvenmeksizin IP paket iletimini şifreler. Bu şifreleme desteğini sunan yazıcı üreticiler kullanılacak değerleri müşteri ortamı ile eşleşecek şekilde ayarlayacaklardır. Kullanılacak kimlik doğrulama yöntemi önceden paylaşılan anahtar ve sertifikaları destekleyecektir.



1. **IEEE802.1x Sertifika Standartını Kullanma**

IEEE802.1x, ağ bağlantıları için kullanılacak bir sertifika standardıdır. IEEE802.1x'in etkin olduğu ağ ortamlarında, bağlantı yalnızca önceden ağ sertifikalarına göre sertifikalandırılmış terminallere izin verecek şekilde ayarlanabilir. IEEE802.1x, aşağıdaki şifreleme yöntemlerini destekleyebilir.

* EAP-TLS
* EAP-TTLS
* EAP-FAST
* PEAP(EAP-MS-CHAPv2)

1. **SNMP v3 Aktif Edilmesi**

SNMP, ağ bağlantısı üzerinden çeşitli ağ cihazlarını yönetmek için tasarlanmış bir protokoldür. Yazıcı cihazlarında SNMPv3 etkinleştirildiğinde, bu SNMPv3 protokolü iletimi, bilgileri sızıntılardan koruyacak şekilde şifrelenir. SNMP V1 ve v2’de bilinen kritik düzeyde zafiyetlr olduğu için SNMP v3 tercih edilmelidir.

1. **IP Adreslerinin Cihazlara Erişiminin Kısıtlanması**

Cihazların arayüz ve terminal erişimlerini güvende tutmak için belirli bir departman veya grubun PC'lerine ayarlanması gerekiyorsa, bu bölümlere veya gruplara ait olmayan kullanıcılardan erişim, etkin IP adres filtrelemesiyle reddedilmelidir.

1. **Gereksiz Protokol ve Servislerin Engellenmesi**

Yazıcılar birçok iletim protokolünü destekler. Bu aktarım protokolleri yeterince güvenli bir şekilde ayarlanmadan etkinleştirilirse, sistemlere Port taraması veya yetkisiz erişimler tarafından saldırı girişimlerine maruz kalabilir. Kullanılmayan aktarım protokollerini devre dışı bırakmayı ve bağlantı noktalarını kapatmak saldırganların sızma girişimlerinde kullanacakları deneme yollarını mümkün olabildiğince kısıtlayacaktır.

1. **Kullanıcı Verilerinin Korunması için Genel Prosedürler**
2. **Cihazların Depolama Alanındaki Verilerin Güvenliğinin Korunması**

Yazıcılara monte edilen HDD / SSD’de, taranan görüntü verileri, önceden basılmış görüntü verileri, kullanıcı kayıt bilgileri veya adres defteri gibi kullanıcı bilgileri saklanır. Bu verileri korumak için, aşağıdaki özellikler uygulanır.

* *HDD / SSD'nin Şifrelemesi*

HDD / SSD’de depolanacak verileri şifrelemek önemlidir. Bunun yapılması verilerin yorumlanması bir PC analiz aracına bağlı olsa bile mümkün kılmamaktadır. Şifreleme algoritması olarak ise simetrik şifreleme algoritması olan AES 256 bit'in tercih edilmesi önerilir.

1. **Cihazda İşlenen Tüm Verileri Silme**

Yazıcılarda kopyalama veya tarama işi yapıldığında görüntü verileri geçici olarak sistemde saklanır. İşi tamamladıktan sonra bilgiler, anlamsız verilerin üzerine yazılarak tamamen silinir ise verilere erişim riski ortadan kalkar. Bunun için cihazın depolama aygıtlarında üreticilerin desteklediği yöntemler (DoD 3 kez silme, Gutmann 35 kez silme) uygulanarak veriler rastgele 0 ve 1 bitleriyle yazılarak geriye doğru dönüştürülmeleri engellenebilir.

1. **İletilen Verilerin Korunması ile İlgili Prosedürler**
2. **Şifrelenmiş Veri İletimi (SSL/TLS)**

Protokollerin SSL / TLS ile şifrelenmesi, taranan bilgileri gönderirken araya girme (MITM) gibi atak vektörlerinden meydana gelebilecek veri sızıntılarının önüne geçer.

1. **Parolalı PDF Dosya İletimi**

PDF Dosyaları içerdikleri verilerin kritikliğiyle orantılı olarak, alıcının bilgileri görüntülemek için parola kullanmasını gerektiren parola korumalı bir PDF göndermenizi sağlar. Bu özellikle, bilgileri taramak, göndermek ya da saklamak için bir parola eklemek dokümanların güvenliğini sağlayacaktır.

1. **Kullanıcı Doğrulama / Erişim Kontrolü**
2. **Kullanıcı Doğrulama**

Kullanıcı doğrulama özelliği, yöneticilerin yazıcılardaki kullanıcıların aktivitelerini yönetmelerine ve tüm aktiviteleri tanımlamasına izin verir. IT yönetimi yetkili kullanıcıların erişim için kayıtlı olmalarına izin verebilir. Genel olarka yazıcılarda doğrulama yapmak için yerel kimlik doğrulama ve ağ kimlik doğrulaması olmak üzere iki doğrulama yöntemi vardır. İkisi de aynı anda kullanılabilir.

* **Yerel Kimlik Doğrulama / Ağ Kimlik Doğrulama**

Yerel kimlik doğrulama, yazıcıya kayıtlı kullanıcı bilgilerini izleyen kimlik doğrulamayı tanımlamak için kullanılan bir yöntemdir. Yerel kimlik doğrulamasında, ayrıntılı kullanıcı yönetimi veya uzaktan yönetim araçlarının erişimi bulunmaz (ssh, rdp vs.). İş kimlik doğrulaması, Kerberos, Active Directory, LDAP vb. mevcut bir kimlik doğrulama sunucusuyla bağlantı kurulur ve kimlik doğrulama yöntemi belirtilir. Ayrıca kullanıcıların kart okuyucu teknolojisiyle bir kart ve şifre birleşimini kullanarak 2 aşamalı bir doğrulama yapmaları da alınabilecek başka bir güvenlik önlemidir.

* **Kullanıcı Hesabı Kilidi**

Yazıcı ağında kullanıcı hesabına girmek için bir kaba kuvvet saldırısı meydana gelirse, belirli bir süre için oturum açmaya çalışırsa, bir oturum açma kimliğinin belirli bir süre için kilitlenebileceği Hesap Kilitleme özelliğini etkinleştirebilirsiniz. Bir hesap için başarısız deneme girişimlerinde hesabın dondurulması için başarısızlıkların sayısı veya süresi belirlenebilir. Ayrıca kaba kuvvet saldırısı genellikle ağ üzerinden gerçekleştirilir. Bu nedenle kilitlenmeye bağlı hesap oturum açma işlemi yalnızca ağdan tüm oturum açma seçeneklerinden seçilebilir.

* **Parola Politikası**

Ağ kimlik doğrulama parolaları dahil, IT tarafından ayarlanmış olmalı ve önceden belirlenmiş olan parolanın minimum uzunluğunu veya şifrenin karmaşıklığını karşılamalıdır (Minimum 8 karakter büyük küçük harf sembolleri rakamlar ve özel karakter barındıran). Parola İlkesi, yerel kimlik doğrulama yöntemi içinde ayarlanabilir.

1. **Erişim Kontrolü**

Erişim Kontrolü ile yazıcıda depolanan veriler veya yazıcı kullanımı, tanımlanmış kullanıcılar tarafından kontrol edilebilir. Bir kullanıcının rolüne bağlı olarak erişim iznini ayarlayarak, dahili bir suç veya bir insan hatası ile bilgi sızıntısı önlenebilir.

* **Doküman Kutularının Aktif Edilmesi**

Bir yazıcı üzerindeki HDD / SSD'de doküman kutuları oluşturularak taranan veriler veya yazdırılan veriler içinde saklanabilir. Kötü niyetli kullanımdan erişimi engellemek için belge kutusuna sadece sahibinin parolası ile erişim aktif edilmelidir.

* **Yetki Ayarları**

Taranan verilerin kopyalanması, yazdırılması, iletilmesi, kutu depolama, harici bellek çalıştırma gibi özellikleri kullanım sınırı her kullanıcı için ayarlanabilir. Kullanım fonksiyonlarını sınırlandırarak yasadışı bilgi sızıntısı veya insan hatası nedeniyle bilgi kaçağı önlenebilir.

1. **Her Bir Fonksiyonu Sınırlandırmak / Yasadışı Kullanımı Önlemek ile İlgili Prosedürler**

Yazıcının çeşitli özellikleri olduğundan, her bir özelliğin yürütülmesi, ayarların düzenlenmesi veya referans yetkisi ayrıntılı olarak belirlenebilir. Ayrıca, bir cihazın yasa dışı kullanımından kaçınmak için, belirli çalışma panellerini kilitlemek ve USB bağlantı noktasını kısıtlamak gibi genel prosedürler uygulanabilir.

* **Kullanıcı Listesi için Düzenleme Otoritesini Ayarlama**

Adres defteri için düzenleme yetkisi ayarı yapılabilir. Otorite kurmanın iki yolu vardır; biri yalnızca bir yönetici yada belirli kullanıcıların belli listeleri yönetme yetkisi atanmasıyla.

* **Kullanıcı Operasyon Paneli Erişim Kısıtlaması**

Bir kullanıcının bir panelden çalışatırabileceği ve erişebileceği kısımların ayarları yapılandırılabilir. operasyon paneli kilidi kullanılarak, bu ayarların çalıştırılması sadece yöneticiye izin verilir. Aşağıdaki kapsamdaki ayarlar panel kilidi için kullanılabilir.

\* Panel Kilidi Açık:

- Sistem menüsündeki tüm işlemler sınırlıdır.

\* Panel Kilit Seviyesi 1:

- Ağ ayarları, sistem ayarları veya belge kutusu ayarları sınırlıdır.

\* Panel Kilit Seviyesi 2:

- Panel 1’deki kısıtlamalara ek olarak panel ayarları, yazıcı ayarları ve iş yürütmeyle ilgili ayarlar sınırlıdır. (Örneğin: Bir durdurma tuşunun kullanılması veya iş iptali vb.)

* **Arayüz Erişim Engellemelerinin Ayarlanması**

Bir aygıta takılı olan USB bağlantı noktasının yasadışı kullanımıyla bilgilerin sızmasını önlemek için, USB bağlantı noktası devre dışı bırakılabilir (engellenebilir).

* **Log Yönetimi**

Log denetim günlükleri yazıcıdan alınıp e-posta yoluyla olarak bildirilebilir. Bu log günlükleri için olaylar giriş / çıkış, iş yürütme, kullanıcı bilgileri veya kutu bilgileri kaydı veya güvenlikle ilgili bilgiler bulunur. Elde edilen günlükler belirtilen bir e-posta adresine iletilebilir. Log kayıtlarına bakarak yasadışı işlem daha sonra izlenebilir. Log günlüğü ayarlarında etkinleştirmek / devre dışı bırakmak, alıcı e-posta adresi ve bir aktarım için kayıt sayısı gibi özellikler aşağıdaki kapsamda ayarlanabilir.

* Giriş Kayıtları
* Yapılan iş kayıtları
* Cihaz geçmiş kayıtları
* Güvenli haberleşme hata kayıtları
* **Düzenli Güvenlik Güncellemelerini Alma**

Yazıcıların düzenli çıkan güvenlik güncelleştirmelerini alıp genel bir ağ yapısıyla hepsine dağıtılması (deploy) önemlidir. Bu güncellemeler güvenlik ve sistemdeki hataların giderilmesi ile akalı olabilir. Bu güncellemelerin takip edilmesi ve toplu yapılması yazıcıların firmwarelerini güncel tutup daha güvenli ve efektif kılacaktır.

|  |  |  |
| --- | --- | --- |
| **#** | **√** | **KONTROL LİSTESİ** |
| **AĞ SERVİSLERİ VE PROTOKOLLERİ** | | | |
| **1** |  | **Listede Verilen Riskli Portlar Firewall Arkasına Alındı mı?** |
| **2** |  | **TCP/IP Protokolleri Haricinde Kullanılmayan Network Servisleri Devre Dışı Bırakıldı mı?** |
| **3** |  | **İlgili Yazıcıya Sabit Bir IP Adresi Atandı mı?** |
| **4** |  | **Mevcutsa Şifreli İletişim Protokollerini (HTTPS, TLS vb.) Kullanın ve Güvenli Olmayan Protokolleri (HTTP vb.) Devre Dışı Bırakın** |
| **5** |  | **Port Haberleşmeleri SSL/TLS Üzerinden Şifrelenerek İletiliyor mu?** |
| **6** |  | **Cihazları DDOS ve Türevi Saldırılara Karşı Korumak İçin ACL ya da Özel bir VLAN’a Alındı mı?** |
| **YÖNETİM** | | | |
| **7** |  | **Yazıcı İçin Büyük Küçük Harf, Özel Karakter ve Rakam Bulunduran Güçlü Bir Yönetici Parolası Oluşturun** |
| **8** |  | **Varsayılan SNMP Topluluk Dizgelerini Güçlü Parolalarla Değiştirin** |
| **9** |  | **Yazıcının Günlük Log Kaydetme Fonksiyonunun Aktif Olduğundan Emin Olun.** |
| **10** |  | **Yazıcı Log Dosyalarının Düzenli Olarak İzlenip İncelendiğinden Emin Olun** |
| **11** |  | **Kimlik Doğrulamayı Aktif Hale Getirerek Adres Defteri, Posta Kutuları ve Log Dosyalarına Erişimi Kısıtlayın** |
| **GÜVENLİK GÜNCELLEŞTİRMELERİ** | | |
| **12** |  | **Yazıcı ile İlgili Yayınlanan Güvenlik Bültenleri Takip Ediliyor mu?** |
| **13** |  | **Yazıcı Üzerinde Mevcut Olan Firmware Yazılımı Belirli Periyotlarla Kontrollü Olarak Güncelleştiriliyor mu?** |
| **FİZİKSEL GÜVENLİK** | | | |
| **14** |  | **Fiziksel Olarak Takılabilen Cihazların (USB Disk, Dongle vb.) Erişimi Kapalı mı?** |
| **15** |  | **Kullanıcıların Konsoldan Taramak, Faks Göndermek veya Kopyalamak için Kimlik Doğrulaması Yapmalarını İsteyin.** |
| **16** |  | **Yazıcının Çıkarılabilir Bir Sabit Sürücüsü Varsa, Cihaza Kilitlendiğinden Emin Olun.** |
| **17** |  | **Mümkünse, Yazdırma Havuzundaki Dosyaları Şifreleyin veya Güvenli Bir Şekilde Silmek İçin Önlemler Alın.** |
| **18** |  | **Güvenlik Politikanızdan Emin Olun, Üreticiye İade İçin Giden veya Diskleri Wipe İşleminden Geçirmeden Göndermeyiniz. Ömrü Dolan ve ya Bozuk Diskleri Güvenli Olarak Öğütünüz (Shredding).** |