Glossar

Fachbegriffe zum Thema Sicherheit

Cyber-Terminologie kann, auch für die Druck-Infrastruktur, komplex sein – und wenn sie nicht verstanden wird, kann dies negative Auswirkungen auf Unternehmen haben. Der Aufbau einer soliden digitalen Verteidigung kann für viele KMU eine große Herausforderung darstellen. Um einen wirklichen Schutz vor Cyber-Bedrohungen zu gewährleisten, müssen Sie das Dickicht aus den entsprechenden Fachbegriffen entwirren – und verstehen. Wir haben nachstehend eine Reihe von Begriffen aus dem Bereich der IT-Sicherheit aufgeführt, um eventuelle Wissenslücken zu schließen.

Active Directory (AD)
Eine Datenbank und eine Reihe von Diensten, die Nutzer mit denjenigen Netzwerkressourcen verbinden, die sie für ihre Arbeit benötigen. Die Datenbank (oder das Verzeichnis (Directory)) enthält wichtige Informationen über die gesamte Umgebung, z.B. welche Nutzer und Computer es gibt und wer was tun darf. Insbesondere wird darüber in der Regel durch die Überprüfung einer eingegebenen Nutzer-ID und eines Kennworts sichergestellt, dass jede Person auch tatsächlich diejenige ist, die sie zu sein vorgibt (Authentifizierung), und sie nur auf die für sie freigegebenen Daten Zugriff hat (Autorisierung).

BIOS
In der Computertechnik ist das BIOS eine Firmware, die Laufzeitdienste für Betriebssysteme und Programme bereitstellt und die Initialisierung der Hardware während des Bootvorgangs durchführt.

Bitdefender Antivirus
Bitdefender ist eine preisgekrönte Anti-Malware-Engine, die den Benutzer vor einer ganzen Reihe von Cyberbedrohungen schützt. Sie ergänzt die nativen Sicherheitsfunktionen der Multifunktionssysteme und schützt vor bekannten und unbekannten Malware-Bedrohungen wie Viren, Trojanern, Würmern, Ransomware, Spyware und persistenten Bedrohungen

Common Criteria
Eine Reihe von Richtlinien, die zur Bewertung von Geräten der Informationstechnologie verwendet werden. Sie sind die technische Grundlage für ein internationales Abkommen, und werden in ihrer Rolle als Spezifikation von unabhängigen Laboren getestet. Die Einhaltung sich entwickelnder Sicherheitsstandards wie Common Criteria ist wichtig, um zu gewährleisten, dass Organisationen sicher mit hochsensiblen Daten auf Sharp Multifunktionssystemen arbeiten können.

Sharp war der erste Hersteller von MFPs und Druckern, der auf das Thema Sicherheit im digitalen Imaging eingegangen ist. Sharp hat die erste Common Criteria-Validierung für ein MFP in 2001 erhalten und wurde als Erster mit einem EAL4-Rating für ein Data Security Kit ausgezeichnet. Zudem erhielt Sharp kürzlich die branchenweit erste Common Criteria-Zertifizierung nach dem aktuellen HCD-PP v1.0-Standard.

Data Security Kit
Das Sharp Data Security Kit hebt die Gerätesicherheit auf ein höheres Niveau mit Funktionen wie dem manuellen Überschreiben von Daten, dem automatischen Überschreiben von Daten beim Einschalten, dem Druck und der Erkennung von versteckten Mustern sowie vielem mehr. Damit ist es möglich, regulatorische Anforderungen zu erfüllen oder spezifische Bedrohungen zu entschärfen. Darüber hinaus sind ausgewählte MFP-Modelle mit einem TPM-Chip ausgestattet, der den unerwünschten Zugriff auf Datenspeicherbereiche, zu denen auch Festplattenlaufwerk (HDD) und Solid-State-Laufwerk (SSD) gehören, verhindert.

SHARP

Glossar

Denial of Service/Distributed Denial of Service (DoS/DDoS)
DoS ist eine Art von Störungsangriff, bei dem der normale Betrieb oder Dienst eines Netzwerks oder Geräts blockiert oder gestört wird. DDoS bezeichnet einen DoS-Angriff, bei dem mehrere (zahlreiche) angreifende Systeme eingesetzt werden, um den Netzverkehr zu verstärken, wodurch die Zielsysteme oder -netze überflutet und möglicherweise überschwemmt werden.

End-of-Lease-Funktion
Wenn ein Multifunktionsdrucker ausgemustert wird, ist es wichtig, dass die im Gerät gespeicherten Daten entfernt oder in ein unlesbares Format gebracht werden. Sharp MFPs bieten standardmäßige End-of-Lease-Funktionen, um sicherzustellen, dass alle vertraulichen Daten überschrieben werden, bevor das Modell die Einrichtung oder die Kundenumgebung verlässt. Einmal gestartet, werden die Daten bis zu 10-mal überschrieben. Wenn ein Sharp Data Security Kit installiert oder die Standard-MFP-Sicherheitsfunktion aktiviert ist, werden die Daten mit Zufallszahlen überschrieben

IEEE802.1x
Ein Netzwerkauthentifizierungsprotokoll, das Ports für den Netzwerkzugang öffnet, wenn eine Organisation die Identität eines Nutzers authentifiziert und ihm den Zugang zum Netzwerk gestattet. Die Identität des Nutzers wird auf der Grundlage von Anmeldeinformationen oder eines Zertifikats festgestellt.

Internet Printing Protocol (IPP)
Ein Netzwerkdruckprotokoll, das die Authentifizierung und die Verwaltung von Druckauftragswarteschlangen ermöglicht. IPP wird von den meisten modernen Druckern und Multifunktionssystemen unterstützt und ist standardmäßig aktiviert.

Internet Protocol (IP) Adresse
Jedes Gerät, das mit dem Internet verbunden ist, muss eine eindeutige Nummer (IP-Adresse) haben, um mit anderen Geräten in Verbindung treten zu können. Derzeit gibt es zwei Versionen der IP-Adressierung: IPv4 und eine spätere aktualisierte Version namens IPv6.

Filterung von IP- oder MAC-Adressen
IP- und MAC-Adressen sind eindeutige Nummern, die zur Identifizierung von Geräten im Internet (IP) oder in einem lokalen Netzwerk (MAC) verwendet werden. Die Filterung stellt sicher, dass IP- und MAC-Adressen mit einer „Whitelist“ abgeglichen werden, bevor Geräte eine Verbindung zu Ihrem Netzwerk herstellen können.

Internet Protocol Security (IPSec)
Eine Reihe von Protokollen zur Sicherung der IP-Kommunikation auf der Netzwerkebene. IPsec umfasst auch Protokolle für die kryptografische Schlüsselerstellung.

Kerberos
Ein Sicherheitsprotokoll für Computernetzwerke, das Dienstanfragen zwischen zwei oder mehreren vertrauenswürdigen Hosts über ein nicht vertrauenswürdiges Netzwerk, wie das Internet, authentifiziert. Es verwendet Kryptographie mit geheimen Schlüsseln und eine vertrauenswürdige dritte Partei zur Authentifizierung von Client-Server-Anwendungen und zur Überprüfung der Identität der Benutzer.

SHARP

Glossar

Media Access Control (MAC) Adresse
Die MAC-Adresse eines Geräts ist eine eindeutige Kennung, die einem Network Interface Controller (NIC) zugewiesen wird. Das bedeutet, dass ein an das Netzwerk angeschlossenes Gerät anhand seiner MAC-Adresse eindeutig identifiziert werden kann.

Malware-Angriff
Bösartige Software (Malware) kann als unerwünschte Software bezeichnet werden, die ohne Ihre Zustimmung auf Ihrem System installiert wird. Sie kann sich an einen legitimen Code anhängen und sich verbreiten; sie kann sich aber auch in nützlichen Anwendungen verstecken oder sich über das Internet replizieren.

Man-in-the-Middle (MITM) Angriff
Bei einem MITM-Angriff setzt sich der Angreifer heimlich zwischen zwei Parteien, die glauben, dass sie direkt miteinander verbunden sind und privat miteinander kommunizieren. Der Angreifer „lauscht" und kann auch die Kommunikation zwischen den Parteien verändern.

Netzwerkdienste
Netzwerkdienste erleichtern den Betrieb eines Netzwerks. Sie werden in der Regel von einem Server (auf dem ein oder mehrere Dienste laufen können) auf der Grundlage von Netzprotokollen bereitgestellt. Einige Beispiele sind Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) oder Voice over Internet Protocol (VoIP).

Persistent Threats (Hartnäckige Bedrohungen)
Eine hochentwickelte, anhaltende Bedrohung (Advanced Persistent Threat, APT) ist ein gut ausgerüsteter Hacker, der ausgeklügelte, böswillige Cyber-Aktivitäten durchführt, die auf ein längeres Eindringen in das Netz bzw. das System abzielen. Zu den Zielen von APTs können Spionage, Datendiebstahl und die Störung oder gar Zerstörung von Netzen und Systemen gehören.

Phishing-Angriff
Phishing ist eine betrügerische Praxis, bei der E-Mails verschickt werden, die vorgeben, von seriösen Unternehmen zu stammen, um Einzelpersonen dazu zu bringen, persönliche Daten wie Passwörter und Kreditkartennummern preiszugeben.

Ports
Ports werden von vernetzten Geräten (PCs, Servern, Druckern, usw.) für die Kommunikation untereinander verwendet (z.B. ein Arbeitsplatzrechner, der sich mit einem Drucker verbindet). Unbewachte offene Ports und Dienste können von Angreifern genutzt werden, um z.B. Malware hochzuladen.

Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0)
HCD-PP v1.0 (vom 10. September 2015) ist die Anforderung für MFPs, die auf den Sicherheitsanforderungen der US-amerikanischen und der japanischen Regierungen basiert und die aktuellste Sicherheitsvalidierung für Unternehmen, Behörden und Militäreinrichtungen bietet. Sie zielt darauf ab, die von einem MFP verarbeiteten Informationen vor Sicherheitsbedrohungen zu schützen und enthält Spezifikationen für Verschlüsselung und Firewalls.

SHARP

Glossar

Protocols (Protokolle)
Ein Protokoll ist definiert als eine Reihe von Regeln und Formaten, die es Informationssystemen ermöglichen, Informationen auszutauschen. In einem Netzwerkkontext gibt es zum Beispiel die Protokolle IP und TLS/SSL.

Ransomware
Als Ransomware bezeichnet man Malware, die User vom Computer aussperrt, oder den Zugriff auf Dateien und Anwendungen blockiert. Ransomware verlangt von Betroffenen die Zahlung einer bestimmten Gebühr (Lösegeldzahlung) als Gegenleistung für einen Entschlüsselungscode, mit dem wieder Zugriff auf Computer oder Dateien ermöglicht wird.

Single Sign-On (SSO, Einmalanmeldung)
Ausgewählte Sharp MFPs bieten Optionen für Single Sign-On, um die Bedienung zu vereinfachen und gleichzeitig den Nutzerzugriff auf den Multifunktionsdrucker und das Netzwerk zu validieren. Wenn ein MFP einer Domain beitritt, baut das MFP vertrauenswürdige Verbindungen zu Netzwerkressourcen auf. IT-Administratoren können sichere, auf Token basierende Kerberos SSO für Netzwerk- und Privatordner sowie Microsoft® Exchange Server bereitstellen. Für den Online-Speicherdienst Google Drive™, den Webmail-Dienst Gmail™ und ausgewählte Cloud-Dienste wird ein OAuth-Token zur Einrichtung von SSO verwendet.

Secure/Multipurpose Internet Mail Extensions (S/MIME)
Eine Reihe von Spezifikationen für die Sicherung von E-Mails. S/MIME basiert auf dem weit verbreiteten MIME-Standard und beschreibt ein Protokoll zur Erhöhung der Sicherheit durch digitale Signaturen und Verschlüsselung.

Spoofing-Angriff
Bei einem Spoofing-Angriff gibt sich eine Partei als ein anderes Gerät oder ein anderer Nutzer in einem Netzwerk aus, um Angriffe auf Netzwerkhosts zu starten, Daten zu stehlen, Malware zu verbreiten oder Zugangskontrollen zu umgehen.

Spyware
Jede Software, die über die Internetverbindung des Users ohne dessen Wissen heimlich Informationen über ihn sammelt (in der Regel zu Werbezwecken) wird als Spyware bezeichnet. Nach der Installation überwacht die Spyware die Aktivitäten des Benutzenden im Internet und überträgt diese Informationen im Hintergrund an eine andere Person. Spyware kann auch Informationen über E-Mail-Adressen und sogar Passwörter oder Kreditkartennummern sammeln.

User installieren das Spyware-Produkt unwissentlich, wenn sie etwas anderes installieren. Eine gängige Methode, Opfer von Spyware zu werden, ist das Herunterladen bestimmter Peer-to-Peer-Produkte für den Dateiaustausch (Filesharing), die heute erhältlich sind.

Spyware entzieht dem Benutzenden Speicherressourcen und verbraucht Bandbreite, da sie Informationen über die Internetverbindung des Users an die Homebase (Ausgangsbasis) der Spyware zurücksendet. Daher können Anwendungen, die im Hintergrund laufen, zu Systemabstürzen oder allgemeiner Instabilität des Systems führen.

Glossar

Transport Layer Security/Secure Sockets Layer (TLS/SSL)
Eine Technologie, die Daten verschlüsselt, wenn sie zwischen zwei Geräten transportiert oder übertragen werden, um ein Abhören bzw. einen Fremdzugriff zu verhindern. TLS/SSL wird häufig für Websites verwendet, kann aber auch zum Schutz anderer Dienste eingesetzt werden.

Trojaner
Ein zerstörerisches Programm, das sich als harmlose Anwendung tarnt. Im Gegensatz zu Viren replizieren sich „Trojanische Pferde" nicht selbst, können aber genauso verheerend sein. Eine der heimtückischsten Arten von Trojanischen Pferden ist ein Programm, das vorgibt, Ihren Computer von Viren zu befreien, stattdessen aber Viren auf Ihren Computer einschleust.

Trusted Platform Module (TPM)
Ein Computerchip nach Industriestandard, der die Kryptoprozessortechnologie nutzt, um Hardware wie Festplattenlaufwerke und Solid State-Laufwerke in MFPs und Druckern zu schützen. Wenn ein Sharp Multifuktionsdrucker mit einem Datensicherheitskit oder TPM installiert wird, initiiert der TPM-Chip einen kryptografischen Schlüssel, auf den die Software nicht zugreifen kann. Ein passender kryptografischer Schlüssel wird während des Bootvorgangs kodiert. Wenn die beiden Schlüssel nicht übereinstimmen, wird der Zugriff auf das Gerät verweigert.

Virus-Detection-Kit
Das Virus-Detection-Kit ist eine optionale Erweiterung für Sharp MFPs mit prämiertem CR5-Controller und schützt vor Malware-Bedrohungen wie Viren, Trojanern, Würmern, Ransomware und Spyware. In Kooperation mit der Firma Bitdefender entwickelt, erreicht das Virus-Detection-Kit eine beispiellose Erkennungsgenauigkeit.

Whitelist
Eine Whitelist ist eine Liste von ausgewählten Personen, Einrichtungen, Anwendungen oder Prozessen, denen besondere Berechtigungen oder Zugriffsrechte erteilt werden. Im geschäftlichen Sinne könnte es sich dabei beispielsweise um die Mitarbeitenden einer Organisation und ihre Rechte für den Zugriff auf das Gebäude, das Netzwerk und ihre Computer handeln. In einem Netzwerk oder Computer kann eine Whitelist Anwendungen und Prozesse definieren, die das Recht haben, auf Datenspeicher in sicheren Bereichen zuzugreifen.

Worms (Würmer)
Ein Programm, das sich selbst über ein Netzwerk verbreitet und sich dabei selbst reproduziert. Es kann sich aber nicht mit anderen Programmen verbinden.

Stand: 11/23, Update: 06/25 | D30 Glossar-Sicherheit-DE-V01-25

SHARP BUSINESS SYSTEMS DEUTSCHLAND GMBH
Industriestraße 180, D-50999 Köln
Tel.: +49 2236 323 100
www.sharp.de

SHARP