



Schützen Sie sich vor The Wolf

Sicherheitsrisiken in den Filmen der „The Wolf“-Serie und
HP Lösungen

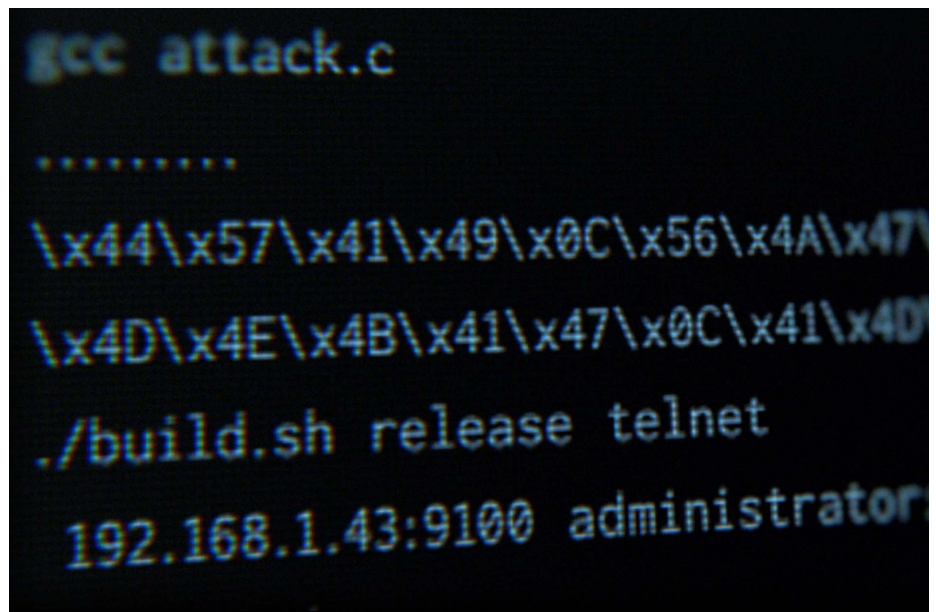
Firewalls alleine bieten keinen ausreichenden Schutz vor den raffinierten Angriffen von Hackern wie The Wolf. Ihr Unternehmen muss den Schutz auf mehrere Ebenen und auf jedes Netzwerk-Endgerät in Ihrer Infrastruktur ausweiten. Tragen Sie mit Sicherheitslösungen von HP zum Schutz Ihrer Geräte, Daten, Identitäten und Dokumente bei.

Staffel 1 The Wolf

Im ersten Film bringt The Wolf einen internationalen Finanzkonzern zu Fall, indem er Schwachstellen von Endgeräten ausnutzt. Er verschafft sich über ein Mobilgerät Zugriff auf einen Drucker und schleust darüber Malware in das Unternehmensnetzwerk ein, um Daten abzufangen und zu lesen. Dann bringt er eine Mitarbeiterin mithilfe einer Phishing-E-Mail dazu, böswilligen Code, der in einer Druckdatei verborgen ist, an einen Drucker zu senden.

Die Malware auf dem Drucker umgeht die Firewall und infiziert die PCs des Unternehmens. Der Code nistet sich auf BIOS-Ebene ein, sodass er fortlaufend Daten weiterleitet und sich nach der Implementierung von Netzwerkschutzmaßnahmen sogar selbst reaktivieren kann.

Zu guter Letzt entdeckt The Wolf noch ein vertrauliches Dokument, das im Ausgabefach eines MFPs liegen gelassen wurde. Der öffentlich bekannt gewordene Verlust sensibler Daten hat für das Unternehmen einen enormen finanziellen Schaden und Ansehensverluste zur Folge.



Schwachstellen

- Die Wi-Fi- oder Bluetooth®-Zugänge von Druckern sind offen und ohne Benutzerauthentifizierung zugänglich.
- Dateien mit Druckerdaten werden nicht verschlüsselt.
- Benutzer erkennen verdächtige E-Mails oder Druckdateien nicht.
- Drucker und PCs sind nicht gegen Malware geschützt.
- Im Ausgabefach von Druckern zurückgelassene Dokumente können vertrauliche Informationen preisgeben.

Wie können Sie sich vor ähnlichen Angriffen schützen?

Schützen Sie Ihre Daten: Deaktivieren Sie die Wi-Fi-/Bluetooth-Funktion oder richten Sie Authentifizierungsverfahren ein. Setzen Sie eine Authentifizierungs- und Verschlüsselungslösung für die mobile Nutzung ein, beispielsweise HP JetAdvantage Connect oder HP Access Control.

Schützen Sie Ihre Geräte: Führen Sie ein Upgrade auf HP Elite-PCs und HP Enterprise-Drucker durch. Diese bieten Schutz vor Malware und ermöglichen das automatische Erkennen und Abwehren von sowie das Wiederherstellen nach Angriffen, ohne dass die IT-Abteilung eingreifen muss. Mit HP Sure Start können Geräte Fehler durch einen Neustart mit einer intakten BIOS-Kopie automatisch beheben.

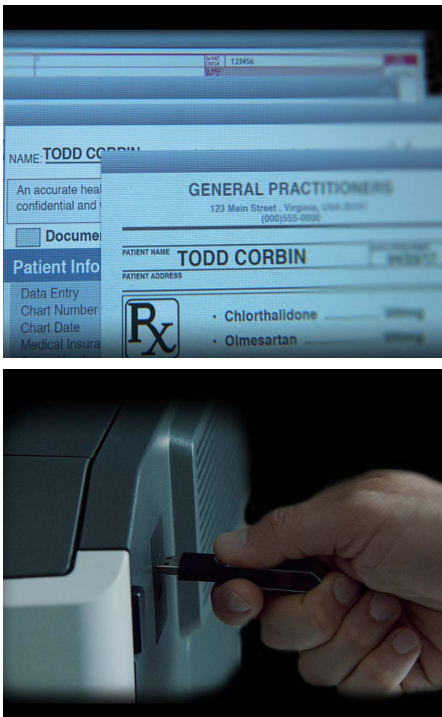
Schützen Sie Ihre Dokumente: Implementieren Sie eine Pull-Printing-Lösung wie HP Access Control oder HP JetAdvantage Secure Print.

Staffel 2 The Wolf: Die Jagd geht weiter

Im zweiten Film hat es The Wolf auf Patientenakten abgesehen, die von einem der weltweit größten Unternehmen für medizinische Software gespeichert werden. Er hackt einen PC und später einen Drucker in einem Krankenhaus, indem er über den USB-Anschluss des Druckers Malware hochlädt.

Da der ungeschützte Drucker mit dem Netzwerk verbunden ist, gelangt die Malware direkt hinter die Firewall und kann nach anderen vernetzten Geräten suchen, um sie zu infizieren. Und weil sich der Drucker in einem nicht segmentierten Netzwerk befindet, kann The Wolf auf Server zugreifen, die mit Datenbanken mit sensiblen Informationen verbunden sind. Er stiehlt Millionen vertraulicher Patientenakten.

Sowohl das Krankenhaus als auch das Software-Unternehmen haften für den Schaden und müssen mit beträchtlichen Geldbußen rechnen.



Schwachstellen

- PCs werden nicht gesperrt, wenn die Benutzer ihren Arbeitsplatz verlassen.
- USB-Anschlüsse von Druckern können ohne vorherige Authentifizierung genutzt werden.
- Datendateien werden nicht verschlüsselt.
- Drucker und PCs sind nicht gegen Malware geschützt.
- Drucker werden nicht auf Sicherheitsbedrohungen überwacht.

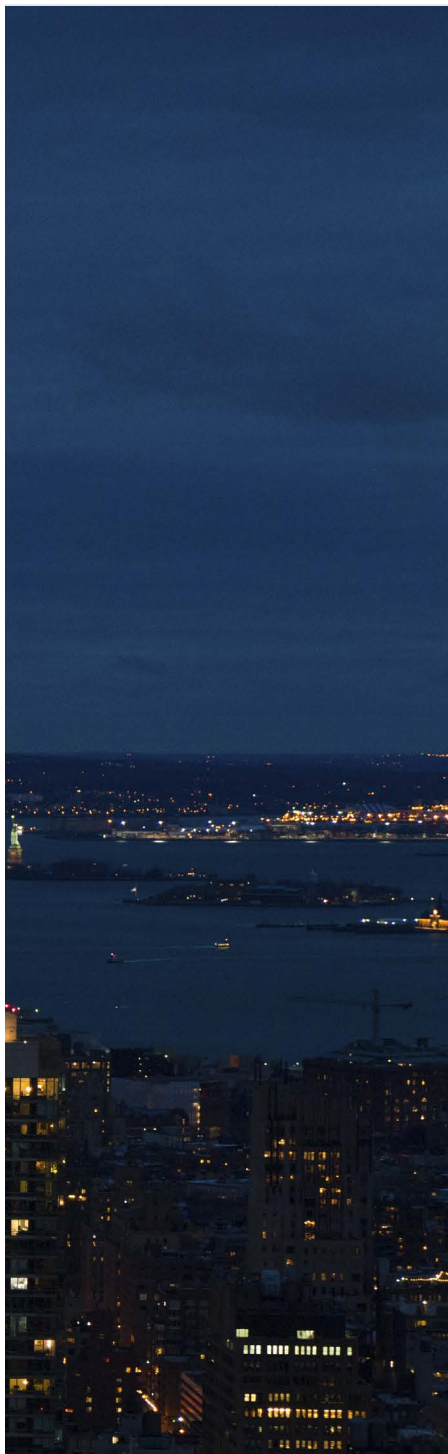
Wie können Sie sich vor ähnlichen Angriffen schützen?

Schützen Sie Identitäten: Verwenden Sie eine mehrstufige Authentifizierung auf HP Elite-PCs.

Schützen Sie Ihre Daten: Setzen Sie eine Authentifizierungs- und Verschlüsselungslösung für Drucker ein, beispielsweise HP Access Control. Deaktivieren Sie nicht verwendete Anschlüsse mithilfe von Benutzersteuerungen. Verwenden Sie eine starke Verschlüsselung für alle Daten während der Speicherung und Übertragung.

Schützen Sie Ihre Geräte: Führen Sie ein Upgrade auf HP Elite-PCs und HP Enterprise-Drucker und -MFPs durch. Diese bieten mit HP Sure Start integrierten Schutz vor Malware zur Abwehr von Angriffen sowie Sicherheitsfunktionen für Integritätsprüfungen bis zur BIOS-Ebene mit automatischer Fehlerbehebung.

Verbessern Sie die Überwachung und Verwaltung: Stellen Sie HP JetAdvantage Security Manager (Drucker) und Manageability Integration Kits¹ (PCs) für die flottenweite automatische Konfiguration von Sicherheitseinstellungen bereit. Erfassen Sie Syslog-Daten, um Sicherheitsvorfälle zu protokollieren. Verbinden Sie Drucker mit SIEM-Tools (Security Information and Event Management), die Sie bei Angriffen in Echtzeit benachrichtigen.



Schützen Sie Ihr Unternehmen mit den umfassenden Sicherheitsfunktionen von HP

Die weltweit höchste Drucksicherheit²

HP Enterprise-Drucker und -MFPs ermöglichen mithilfe von Funktionen wie der Angriffserkennung für die Laufzeitumgebung und HP Sure Start das automatische Erkennen und Abwehren von sowie das Wiederherstellen nach Angriffen, ohne dass die IT-Abteilung eingreifen muss. Darüber hinaus können Sie weitere Schutzmaßnahmen wie verschlüsselte Festplatten, erweiterbare Firmware und die Möglichkeit zum Senden von Sicherheitswarnungen an SIEM-Tools nutzen.

hp.com/go/PrintersThatProtect

Die weltweit sichersten und verwaltungsfreundlichsten PCs³

HP Elite-PCs bieten Rundumschutz für das Betriebssystem vor den am häufigsten auftretenden Bedrohungen. HP Multi-Factor Authenticate bietet zusätzlichen Schutz für Identitäten und das HP Manageability Integration Kit¹ vereinfacht die Verwaltung der Sicherheit für die gesamte PC-Flotte.

hp.com/go/ComputerSecurity

HP JetAdvantage Connect

Nutzen Sie vorhandene IT-Netzwerktools und Richtlinien, um Druckvorgänge über Smartphones und Tablets zu verwalten und den Benutzern das sichere Drucken wie von einem PC aus zu ermöglichen – ganz ohne App.

hp.com/go/JetAdvantageConnect

HP Access Control

Durch Funktionen für rollenbasierte Druckauthentifizierung, Autorisierung und sicheres Pull-Printing im gesamten Unternehmen können Sie die Kontrolle zurückerlangen, die Sicherheit verbessern und die Kosten senken.

hp.com/go/hpac

HP JetAdvantage Secure Print

Schützen Sie vertrauliche Dokumente mit cloudbasiertem Pull-Printing. Benutzer authentifizieren sich am Drucker ihrer Wahl, um ihre Druckaufträge abzurufen und zu drucken.

hp.com/go/JetAdvantageSecurePrint

HP JetAdvantage Security Manager

Reduzieren Sie die Kosten und den Ressourcenbedarf für die Flottensicherheit mit dem branchenweit einzigen richtlinienbasierten Compliance-Tool für Drucksicherheit.⁴ Sie können damit für Ihre gesamte Druckerflotte Sicherheitsrichtlinien festlegen, die Behebung von Gerätefehlern automatisieren, spezielle Zertifikate installieren und verlängern sowie Compliance-Berichte erstellen.

hp.com/go/securitymanager

Weitere Informationen unter

hp.com/go/hpsecure

¹ HP Manageability Integration Kit ist nicht vorinstalliert, verfügbar unter hp.com/go/clientmanagement.

² Basierend auf einer von HP durchgeführten Prüfung der im Jahr 2016 veröffentlichten Angaben zu Sicherheitsfunktionen von vergleichbaren Druckern von Wettbewerbern. Nur HP bietet eine Kombination aus Sicherheitsfunktionen, die durch Überwachung einen Angriff erkennen und automatisch stoppen und danach bei einem Neustart die Integrität der Software eigenständig prüfen können. Eine Liste der Drucker finden Sie hier: hp.com/go/PrintersThatProtect. Weitere Informationen: hp.com/go/printersecurityclaims.

³ Basierend auf den einzigartigen und umfassenden Sicherheitsfunktionen von HP (ohne zusätzliche Kosten) und den Verwaltungsfunktionen des HP Manageability Integration Kit für alle PC-Bereiche, inklusive der Verwaltung von Hardware, BIOS und Software mit Microsoft® System Center Configuration Manager bei Anbietern mit jährlich mehr als 1 Mio. verkauften Einheiten (Stand November 2016) auf HP Elite PCs mit Intel® Core®-Prozessoren der 7. Generation, integrierten Intel®-Grafikkarten und Intel® WLAN.

⁴ Wettbewerbsaussage basierend auf internen HP Untersuchungen in Bezug auf Lösungen anderer Anbieter (Device Security Comparison, Januar 2015) und dem Solutions Report zu HP JetAdvantage Security Manager 2.1 von Buyers Laboratory LLC, Februar 2015. Weitere Informationen finden Sie unter hp.com/go/securitymanager.

Melden Sie sich noch heute an
hp.com/go/getupdated



An Kollegen weiterleiten

