GRÜNDE FÜR DIE WICHTIGKEIT EINER SICHERHEIT AUF MEHREREN EBENEN

Firewall
Antivirenprodukt
Proaktive Verteidigung gegen Schadsoftware
Beseitigung von Schadsoftware
Benutzer-schulung

WAS IST SICHERHEIT AUF MEHREREN EBENEN?

Verschiedene Lösungen für die Cyber-Sicherheit arbeiten zusammen, um die Angriffsfläche eines vernetzten Systems zu reduzieren.

WORIN BESTEHEN DIE NEUESTEN HERAUSFORDERUNGEN?

Die Mehrheit der IT-Administratoren und CSPs (Cyber Security Practitioner) ist der Ansicht, dass das Endpunktrisiko aus folgenden Gründen erheblich gestiegen ist:

73 % Nutzung von gewerblichen Cloud-Anwendungen

63 % Mitarbeiter arbeiten zu Hause oder an dezentralen Standorten

68 % Nutzung von mitarbeitereigenen Mobilgeräten

HÄUFIGSTE ARTEN VON ANGRIFFEN

Schadsoftwareangriffe auf IT-Netzwerke im vergangenen Jahr (mehrere Antworten zulässig):

- **80 %** Schadsoftwareangriffe aus dem Internet
- **65 %** APTs / gezielte Angriffe
- **65 %** Rootkits
- **55 %** Spear-Phishing-Angriffe

ZUNAHME AN SCHWERE UND EFFIZIENZ

69 % der Umfrageteilnehmer gaben an, dass die Schwere der Schadsoftwarevorfälle im vergangenen Jahr zugenommen hat.

60 % der Zeit sind Angreifer dazu in der Lage, Organisationen innerhalb von wenigen Minuten zu gefährden[1].

WELCHE LÜCKEN WEIST IHRE VERTEIDIGUNG AUF?

KEINE AKTUELLEN PATCHES

Von den 7 Millionen öffentlich bekannten Informationssicherheits-lücken waren bei den im Jahr 2014 erkannten Exploits nur **10 für fast 97 % der Vorfälle verantwortlich**[2].

99,9 % der Exploits erfolgten mehr als ein Jahr **nach Veröffentlichung der jeweiligen Sicherheitslücke.**

SCHWACHE SICHERHEIT

Zu lange Erkennungszeiten, bekannte Schwachstellen nicht gepatcht, Sicherheitsrichtlinien nicht durchgesetzt oder bekannte, fehlende oder schlecht umgesetzte Verschlüssel-ung, kein Schutz vor Schadsoftware, schwache Wireless-Konfigurationen, Schwachstellen bei der physischen Sicherheit, unstrukturierte Informationen, veraltete Anwendungen, die nicht mehr unterstützt werden, Anbieter und Geschäftspartner, die möglicherweise nicht vollständig sicher sind.

UNACHTSAME ODER NICHT INFORMIERTE BENUTZER

- Opfer von Phishing-Angriffen und anderen Social-Engineering-Taktiken
- Umgehung von Sicherheitsvorkehrungen und Installation von Schadsoftware direkt auf dem System
- Preisgabe von Zugriffsinformationen bei Phishing-Angriffen
- Einstellung von Sicherheitsinformationen auf sozialen Medien

WELCHE EBENEN BRAUCHEN SIE?

Technologielösungen

Software zum Schutz vor Angriffen
Bogenschützen: Beinhaltet Technologie zum Schutz vor Exploits, Spam und Phishing. Technologie zum Schutz vor Exploits kann schädliche Programme deaktivieren, bevor Angreifer in das System eindringen können.

Netzwerk
Burg: Eine vollständig aktualisierte und gepatchte Betriebssystemsoftware trägt zu einem sicheren Netzwerk bei.

Firewall
Burgmauer: Beinhaltet IP-Positivlisten, IP-Negativlisten und IP-Portsicherheit. Grenzt die Außenwelt vom internen Netzwerk ab.

Antischadsoftware
Ritter: Bekämpft neue Bedrohungen und bereinigt Infektionen. Erkennt außerdem unerwünschte Software wie PUPs und hindert diese daran, Spam an Benutzer zu senden oder deren Systemressourcen zu belasten.

Herkömmliches Antivirenprodukt
Wächter: Verhindert Infektionen durch Viren, Trojaner, Würmer und andere bekannte Bedrohungen.

Mit dem Internet verbundene Anwendungen
Burgtore: Apps wie Java und Flash machen das Netzwerk angreifbar, wenn sie nicht aktualisiert werden.

Lösungen zur Steigerung des Bewusstseins

Sind meine Cyber-Richtlinien dokumentiert?

Sind sie angemessen?

Befolgen meine Mitarbeiter die Richtlinien?

Verwende ich Technologien zur Unterstützung dieser Richtlinien?

Der IT-Administrator sammelt Bedrohungs-informationen aus externen Quellen und nutzt diese zur Abwehr von Angriffen.

Er wahrt die Sicherheit der Benutzer außerdem durch starke Richtlinien.

Der Benutzer ist die WICHTIGSTE SICHER-HEITSVORKEHRUNG.

Ein gut informierter Benutzer stärkt alle anderen Sicher-heitsebenen.

Weitere Informationen finden Sie unter **malwarebytes.org/articles**

Malwarebytes

Quellen: 1. 2015 State of the Endpoint Report: User-Centric Risk, im Auftrag von Lumension, unabhängig durchgeführt von Ponemon Institute LLC (Jan. 2015); Verizon 2015 Data Breach Investigations Report
2. Verizon 2015 Data Breach Investigations Report