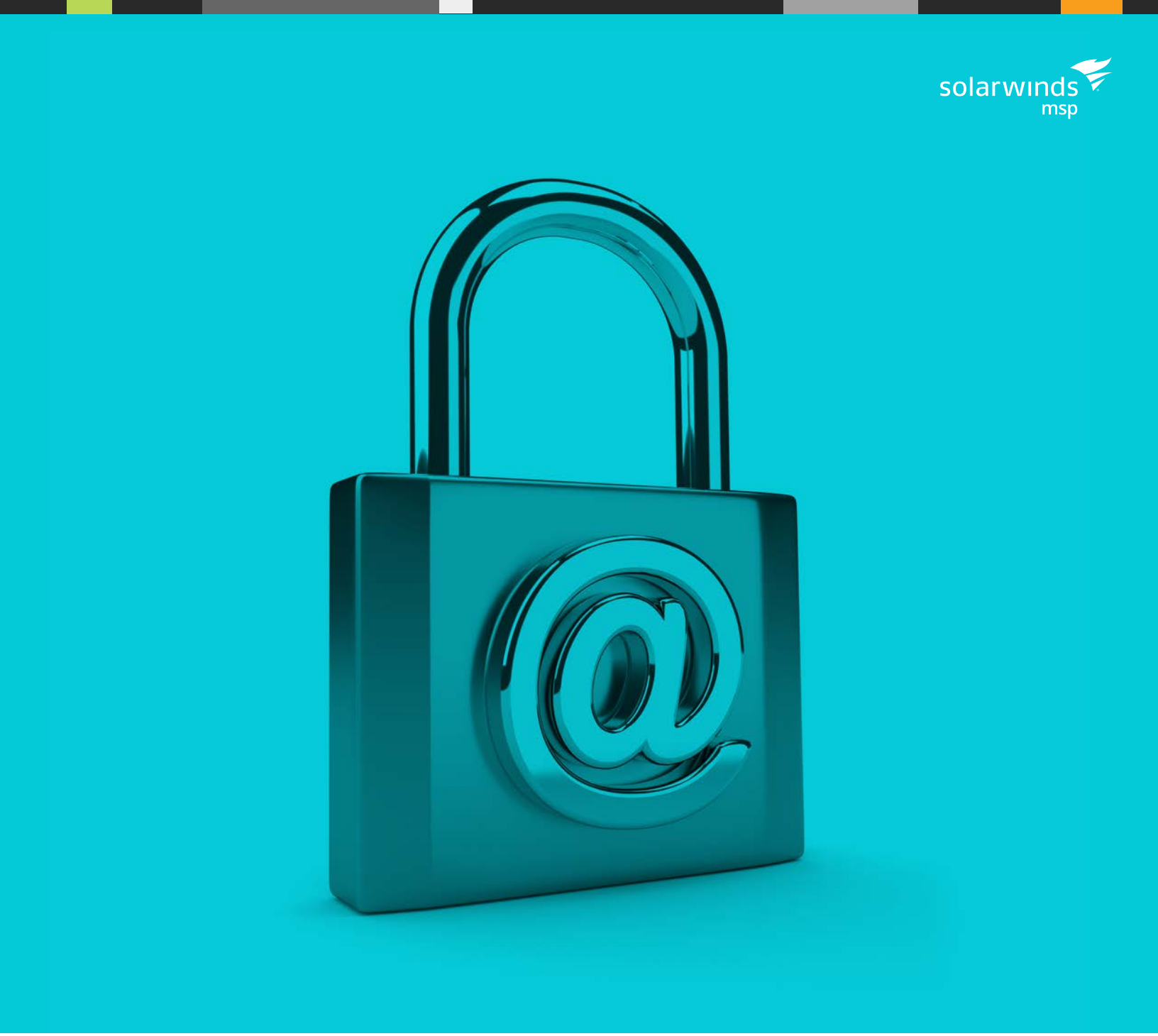
solarwinds msp



E-Book

Sichere E-Mails, reibungsloser Geschäftsbetrieb

BESONDERS ANFÄLLIG FÜR HACKERANGRIFFE: E-MAIL

E-Mail ist weithin der wichtigste geschäftlich genutzte Dienst – das wird anhand der rasanten weltweiten Wachstumsraten deutlich. Laut einem Bericht von Radicati zur Entwicklung des E-Mail-Aufkommens zwischen 2017 und 2021 gab es im Jahr 2017 gut 6,3 Milliarden E-Mail-Konten und ihre Zahl wird bis 2021 voraussichtlich auf über 7,7 Milliarden steigen. Die meisten E-Mails sind laut dem Bericht geschäftlicher Natur – wurden im Jahr 2017 täglich 269 Milliarden geschäftliche E-Mails verschickt, so sollen es bis 2021 319,6 Milliarden werden. E-Mails sind das Herzstück der Unternehmenskommunikation.

Der Nachteil des Kommunikationskanals E-Mail: Er lässt sich zu kriminellen Zwecken missbrauchen. Mitarbeiter erhalten ungezählte Spam-Mails mit unverdächtig wirkendem, jedoch schädlichen Anhängen, die allzu leicht einzelne Computer oder gar gesamte Unternehmensnetzwerke infizieren können. Fast 70 % aller weltweit verschickten E-Mails sind Spam oder Malware. Die über SolarWinds® Mail Assure™ gesammelten Daten bestätigen diese Zahl.

DIE ÜBLICHEN METHODEN BEI ANGRIFFEN AUF E-MAIL-SYSTEME

- **Pufferüberlauf** – Tritt unter Umständen auf, wenn auf einem E-Mail-Server sehr viele Daten gleichzeitig eintreffen.
- **Phishing** – Bei dieser Spamvariante werden E-Mail-Empfänger im Unternehmen auf die eine oder andere Weise dazu gebracht, den Zutritt zum Unternehmensnetzwerk zu ermöglichen. Phishing-Mails fordern zu bestimmten Handlungen auf und stammen angeblich von einem vertrauenswürdigen Absender. So könnte die IT-Abteilung des eigenen Unternehmens beispielsweise darum bitten, sich auf einem bestimmten Webportal anzumelden. Die dahintersteckende betrügerische Website sammelt die eingegebenen Anmeldedaten, mit denen die Angreifer sich dann Zutritt ins Unternehmensnetzwerk verschaffen können.
- **Massenhafter Ein- und Ausgang von E-Mails** – Bei hohem E-Mail-Aufkommen werden die Nachrichten vor Zustellung zum lokalen Mailserver gefiltert, um Bandbreite zu sparen und den Server bei der Verarbeitung relevanter E-Mails zu entlasten.
- **Denial of Service (DoS)** – Treffen E-Mails in großer Menge auf ein DSL- oder Kabelmodem mit geringer Bandbreite, so zieht dies extern gehostete Dienste in Mitleidenschaft und macht andere Internetdienste wie VPN oder Remote Desktop unbrauchbar.

Im Oktober 2013 wurden 153 Millionen Adobe-Accounts gehackt – alle enthielten E-Mail-Adressen von Kunden im Klartextformat.

SCHUTZ VOR SPAM UND PHISHING

Im Oktober 2013 wurden 153 Millionen Adobe®-Accounts gehackt* – alle enthielten E-Mail-Adressen von Kunden im Klartextformat. Aufgrund einer schwachen Kennwortverschlüsselungsmethode ließen sich zudem viele Kennwörter leicht entschlüsseln. Wer Adobe-Software aktivieren und lizenzieren möchte, benötigt dafür einen Account auf einem Adobe-Server. Entsprechend schnell hatten die Hacker gültige E-Mail-Adressen ermittelt, an die sie Phishing-Mails und Spam senden konnten. Vorfälle wie dieser zeigen klar: Es gibt dringenden Bedarf, die vielen E-Mail-Konten weltweit vor den Phishing-Angriffen böswilliger Hacker und den sich daraus ergebenden Konsequenzen für Unternehmensnetzwerke zu schützen.

* Quelle: Adobe-Bericht 2016, Seite 12

GEFÄHRLICH: DIREKTVERBINDUNGEN MIT DEM MAILSERVER

Eine der Methoden, mit denen sich Cyberkriminelle Zutritt zu Unternehmensnetzwerken verschaffen, besteht im Aufbau einer direkten Verbindung zum betreffenden E-Mail-Server. Es empfiehlt sich also, durch Regeln einzuschränken, welche IP-Adressen zu einer solchen Verbindung berechtigt sind. Ein auf mehreren Ebenen angelegtes Schutzkonzept hebelt das Ausschnüffeln von Unternehmensnetzwerken per Direktverbindung nahezu vollständig aus.

„Ohne direkte Verbindung zum Mailserver können Hacker unmöglich herausfinden, mit welcher Software der Server betrieben wird, was ein Aufspüren von Schlupflöchern deutlich erschwert. Gerade bei älteren Versionen von Microsoft Exchange auf älteren Geräten mit beschränkter Kapazität ist dieser Punkt enorm wichtig." – Führender MSP, MSP-Unternehmen

Eine der Methoden, mit denen sich Cyberkriminelle Zutritt zu Unternehmensnetzwerken verschaffen, besteht im Aufbau einer direkten Verbindung zum betreffenden E-Mail-Server.

ELEGANT UND SICHER: GEHOSTETER E-MAIL-SCHUTZ

VIELSCHICHTIGER SCHUTZ FÜR E-MAILS

Ein gehosteter E-Mail-Schutzdienst ist der zu schützenden Infrastruktur vorgeschaltet und überwacht, welche IP-Adressen sich mit dem Mailserver zu verbinden versuchen. Über MX-Einträge lässt sich steuern, dass sämtliche E-Mails zuerst an den gehosteten E-Mail-Schutzdienst gehen. Dort werden sie auf Spam, Viren, Ransomware, Phishing, Malware und alle anderen E-Mail-Bedrohungen geprüft und entsprechend gefiltert. Mailserver und Firewall müssen so konfiguriert sein, dass nur eine Verbindung mit dem gehosteten Schutzdienst akzeptiert wird. Beides zusammen wappnet effizient gegen alle Arten von Bedrohungen, denn es stellt sicher, dass nur E-Mails zum lokalen Mailserver durchgelassen werden, die zuvor den Filter des Schutzdienstes passiert haben. Ein weiterer Vorteil dieser Konfiguration besteht in der Möglichkeit zur Überwachung des vom lokalen Mailserver ausgehenden E-Mail-Aufkommens.

Verschickt der Server plötzlich sehr viele Nachrichten, so kann dies auf Netzwerkprobleme an anderer Stelle hindeuten. Ein ausgereiftes E-Mail-Sicherheitssystem bietet außerdem eine Blacklisting-Funktion zum Sperren von Malware-Absendern. So wird wiederum das IP-Blacklisting von Netzwerken verhindert und der gute Ruf der IP-Adresse wird gewahrt.

WASSERDICHT DURCH MEHRERE VERTEIDIGUNGSLINIEN

KEINE CHANCE FÜR ANGREIFER

Eine ausgereifte Schutzlösung bietet gleich mehrere ineinandergreifende Ebenen. Mechanismen wie Viren- oder Webschutz ergänzen den E-Mail-Schutz und ermöglichen eine solide Absicherung von Unternehmensnetzwerken.

Bei mehreren Verteidigungslinien werden Angreifer, die es durch eine Linie geschafft haben, einfach an der nächsten abgewehrt: Lassen Blacklist und Spamfilter versehentlich eine betrügerische E-Mail durch, so gerät ihr Malware-Anhang in die Maschen des Virenscanners. Surfen Mitarbeiter aus dem Unternehmensnetzwerk heraus auf betrügerische Websites, so schlägt der Webschutz Alarm. Alle Maßnahmen gemeinsam bilden eine stählerne Abwehr gegen Gefahren für Netzwerk und Infrastruktur.