SONICWALL

KURZDARSTELLUNG: WARUM SIE RAFFINIERTE BEDROHUNGEN NUR MIT EINER HOCH ENTWICKELTEN E-MAIL-SICHERHEITSLÖSUNG STOPPEN KÖNNEN

Angesichts ausgeklügelter Ransomware und unbekannter Bedrohungen ist das Thema E-Mail-Sicherheit wichtiger denn je

Zusammenfassung

In einer hochgradig vernetzten Welt gehören E-Mails nicht nur zum Alltag – sie bilden die Grundlage für effiziente Geschäftsprozesse. Schätzungen zufolge soll die Menge an E-Mails, die täglich versendet werden, weltweit um mindestens 5 Prozent pro Jahr steigen. Angesichts ihrer enormen Verbreitung sind E-Mails ein beliebtes Vehikel für Hacker, um verschiedenste Bedrohungen einzuschleusen. Das wird sich auch in Zukunft nicht ändern.

E-Mail-Nutzung steigt weiter an

Obwohl Nachrichten-Apps und soziale Medien weiterhin auf dem Vormarsch sind, nimmt auch die E-Mail-Kommunikation stark zu. Einer vor kurzem durchgeführten Untersuchung der Radicati Group zufolge werden weltweit insgesamt 205 Milliarden E-Mails pro Tag versendet und empfangen, wobei diese Zahl voraussichtlich um mindestens 5 Prozent jährlich steigen soll[1]. Dieser Trend ist auch Hackern nicht entgangen. Nach wie vor suchen sie kontinuierlich nach Möglichkeiten, Organisationen anzugreifen.

1 The Radicati Group, Inc., Email Statistics Report, 2015-2019

Anatomie eines E-Mail-Angriffs

- Ein CFO erhält vom CEO per E-Mail die Anweisung, eine dringende Geldüberweisung zu tätigen. In Wahrheit stammt die E-Mail von einem Cyberkriminellen.
- Ein Mitarbeiter mit administrativen Rechten für wichtige Systeme erhält von der IT eine dringende E-Mail mit der Aufforderung, sein Netzwerkpasswort zu aktualisieren. In Wirklichkeit gibt er sein Passwort an Cyberkriminelle weiter.
- Ein Mitarbeiter erhält eine E-Mail mit der Bitte, einen wichtigen Anhang über seinen Leistungsanbieter zu lesen. Wenn er den Anhang öffnet, aktiviert er unwissentlich einen versteckten Trojaner.

Welche E-Mail-Bedrohungen gibt es für Organisationen?

Hacker nutzen E-Mails, um Organisationen auf verschiedene Weisen zu attackieren. Zu den häufigsten E-Mail-Bedrohungen gehören:

- **Malware** – E-Mails sind eine der beliebtesten Methoden, um bekannte und unbekannte Malware zu verteilen. In der Regel wird diese Malware in der Hoffnung, dass der Anhang auf einem Computer oder Netzwerk geöffnet oder heruntergeladen wird, in E-Mail-Anhängen eingebettet. Auf diese Weise können Hacker auf Ressourcen zugreifen, Daten stehlen oder ganze Systeme lahmlegen.
- **Ransomware** – eine besonders böswillige Malware-Variante ist die sogenannte Ransomware. Sobald der E-Mail-Anhang angeklickt wird, nistet sich bösartiger Code im Netzwerk ein. Typischerweise verschlüsselt oder sperrt die Ransomware dann kritische Dateien und Systeme. Die Hacker nötigen die Organisation dazu, ein Lösegeld zu bezahlen, um die Dateien oder Systeme zu entschlüsseln oder zu entsperren.
- **Phishing** – bei dieser häufigen Hacker-Taktik werden E-Mails mit eingebetteten Links verschickt, die auf Hacker-Websites verweisen. Wenn unerfahrene, leicht zu täuschende User diese Sites besuchen, werden sie aufgefordert, personenbezogene Daten einzugeben. Diese Information wird dazu verwendet, Identitäten zu stehlen, an Unternehmensdaten zu gelangen oder auf andere kritische Systeme zuzugreifen.
- **Spear-Phishing / Whaling** – bei dieser Phishing-Variante senden Hacker wichtigen IT-/Netzwerk-Verantwortlichen oder leitenden Angestellten mit Malware infizierte E-Mails aus vermeintlich vertrauenswürdigen Quellen, um sich einen Zugriff auf interne Systeme und Daten zu verschaffen.
- **Business-E-Mail-Compromise / CEO-Fraud / betrügerische E-Mails** – den neuesten Zahlen des FBI zufolge haben in den letzten zwei Jahren rund 22.000 Unternehmen weltweit infolge von Business-E-Mail-Compromise(BEC)-Angriffen Verluste in Höhe von mindestens 3,1 Milliarden USD erlitten[1]. Das FBI definiert Business-E-Mail-Compromise als ausgeklügelten E-Mail-Betrug, der auf Unternehmen abzielt, die mit ausländischen Partnern arbeiten und regelmäßig elektronische Überweisungen tätigen.
- **Spam** – mithilfe von E-Mails werden Spam oder unaufgeforderte Nachrichten verschickt, die Posteingänge und Netzwerkressourcen verstopfen, die Produktivität beeinträchtigen und zusätzliche operative Kosten verursachen.
- **Hijacking ausgehender E-Mails** – firmeninterne Richtlinien und gesetzliche Vorgaben verpflichten Unternehmen dazu, ausgehende E-Mails zu prüfen, um personenbezogene Kundendaten zu schützen. Durch Zombie-Angriffe und IP-Hijacking können personenbezogene Kundendaten in Umlauf gebracht werden, was dem Ansehen des Unternehmens schadet.

Fazit

E-Mails sind ein wichtiges Kommunikationsinstrument moderner Organisationen – das wissen auch Hacker. Um gegen die wachsende Flut hochkomplexer, ausgereifter Bedrohungen gewappnet zu sein, sind mehrschichtige Sicherheitslösungen mit einem speziellen hoch entwickelten E-Mail-Schutz absolut unerlässlich. Organisationen sind daher gut beraten, eine E-Mail-Sicherheitslösung der nächsten Generation zu implementieren, die einen grundlegenden E-Mail-Schutz bietet und auch neueste Bedrohungen effektiv bekämpft.

Sie möchten erfahren, wie Sie Ihre E-Mails effizient schützen können? Dann lesen Sie unsere Lösungsübersicht „Was Ihre Next-Generation-E-Mail-Sicherheitslösung können muss, um hoch entwickelte Bedrohungen zu stoppen“.

1 www.ic3.gov/media/2016/160614.aspx

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com