E-MAIL PROTECT PRO

NEXT GENERATION E-MAIL SECURITY

E-Mail – Das immer noch grösste Einfallstor für Schadprogramme.

Im Jahr 2017 waren rund 53% der weltweit täglichen versandten E-Mails Spam, wovon durchschnittlich 80% mit Schadsoftware versehen waren. Doch dies ist nur ein Teil des Problems. Die Belastung durch Ransomware[1] (z.B. Locky, WannaCry, etc.) und zielgerichtete Angriffe nimmt stetig zu. So sind in 2017 Angriffe mittels Ransomware um 35% und Spear-Phishing[2] Kampagnen um 55% gestiegen. Auch im Jahr 2018 gehört das Eingangstor E-Mail weiterhin zu den beliebtesten Angriffzielen für Hacker: Ein als Anhang einer E-Mail verschickter Virus erweist sich als hartnäckiger und resistenter Schädling, der Unternehmensdaten klaut oder die Festplatte verschlüsselt.

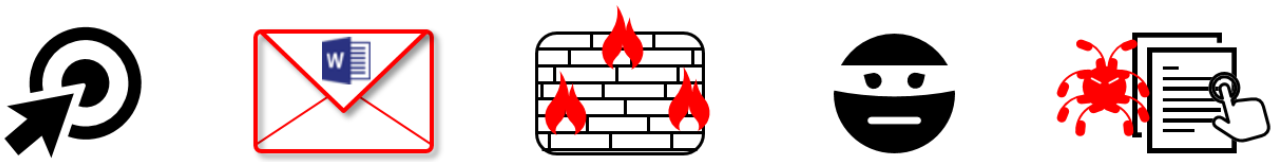
[1] Ransomware ist eine Malware, die Ihren Computer infiziert und all Ihre Daten verschlüsselt. Erst nach einer Lösegeldzahlung werden Ihre Daten vermeidlich wieder freigegeben.
[2] Unter Phishing versteht man Versuche von Hackern, über gefälschte Internet-Seiten oder E-Mails an Benutzer-Daten (z.B. Passwörter) zu kommen.

BEDROHUNGSLAGE

Noch nie zuvor wurden so viele Schadprogamme via E-Mail verteilt wie im Jahr 2017

Angriffskette

So unterschiedlich die Motivation von Angreifern auch sein mögen, sind die Auswirkungen auf Unternehmen die selben. Es entstehen mittelbare und unmittelbare Kosten. Betrachtet man die Vorgehensweise von Hackern vor und während eines Angriffs, so wird erkennbar, dass die Angriffskette (in der Literatur auch „Kill Chain“ genannt) sich in folgende fünf Schritte unterteilen lässt.



INFORMATIONS-BESCHAFFUNG & WEAPONIZATION	ZUSTELLUNG	INITIAL EXPLOITATION	INSTALLATION	EXFILTRATION
Beschaffung von Informationen über das Opfer. Kopplung Exploit mit ggf. personalisiertem Dokument.	E-Mail an Zielperson/ Personenkreis mit gefälschter Absenderadresse und angeblich legitimen Inhalt.	Öffnet der Benutzer den Anhang wird der Exploit durch Ausnutzen von Betriebssystem-Schwachstellen installiert.	Nachladen von weiterer Malware vom Command and Control Server und Ausführung dieser (z.B. Ransomware, Trojaner, etc.).	Das Unternehmen ist infiltriert (z.B. Daten fließen unbemerkt aus dem Unternehmen ab oder Ransomware verschlüsselt Rechner).

Um sich vollumfänglich vor diesen gezielten Angriffen schützen zu können, bedarf es eines Services der mittels mehrstufigen Filtersystems proaktiv Maßnahmen ergreift um Malware zu erkennen und zu blocken.

E-MAIL PROTECT PRO
E-MAIL SECURITY AS A SERVICE

E-Mail Protect Pro schützt mittels seines mehrstufigen Filtersystems vor Spam, mailbasierten DDOS-Angriffen, Spear-Phishing, Spoofing, sowie bekannten und unbekannten Schadprogrammen. Mittels des in deutschen Rechenzentren georedundant aufgebauten Services, garantiert die Telekom eine monatlich durchschnittliche Verfügbarkeit von 99,9%.

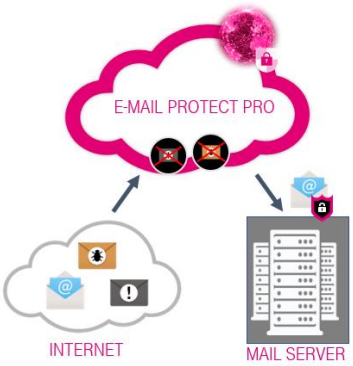
Produktvorteile

- Ohne Software, ohne Hardware und unnötigen Administrationsaufwand (Security as a Service)
- Mehrstufiges Sicherheitssystem
- Entlastung kundeneigener Ressourcen
- Skalierbar, ob 25 Nutzer, 500 oder 100.000 Nutzer
- Verfügbarkeit von 99,9%
- Service rund um die Uhr (24/7/365)
- Anbindung Office 365 (via MX-Record)
- Schutz vor Ransomware und anderen Advanced Persistant Threats
- Malware-Tiefenprüfung auf CPU-Ebene, wo sich Exploits nicht verbergen können
- Security Made in Germany – betrieben in hochsicheren deutschen Rechenzentren

Mit E-Mail Protect Pro gehören teure und komplexe E-Mail Security Lösungen der Vergangenheit an. Die als Security as a Service bereitgestellte Plattform schützt mit einer Verfügbarkeit von 99,9% vor bekannten und unbekannten Gefahren wie z.B. Ransomware oder Zero Day Sicherheitslücken. Um sich vor diesen Gefahren zu schützen muss lediglich der MX-Record des Unternehmens umgeleitet werden.

E-Mail Protect Pro untersucht mittels proaktiver Mechanismen den E-Mail Verkehr zunächst auf Spam und bekannte Viren. Hierbei werden verschiedene Verfahren wie die Prüfung auf RFC Konformität, DNS Checks, Recipient Check, Sender Policy Framework (SPF) und weitere angewendet. Anschließend untersuchen mehrere unabhängige Anti-Viren-Scanner die E-Mails auf bekannte Gefahren. Zusätzliche Sicherheit bietet die Virus Outbreak Detection, die auf Basis heuristischer Analysen signaturunabhängig nach Mustern im E-Mail-Header und Body sucht.

Zum Schutz vor neuartigen und zielgerichteten Angriffen (sogenannten Advanced Persistant Threats) setzt die Telekom Security auf Ihre innovative Technologie „APT Protect Pro“. Dabei werden potenziell schädliche Dateien in einer sicheren, isolierten Umgebung ausgeführt und das Verhalten auf ungewöhnliche Aktivitäten (z.B. Aktualisierungen der Registry, Änderungen der DLLs) analysiert. Im Gegensatz zu herkömmlichen Sandbox-Systemen anderer Anbieter, findet bei APT Protect Pro die Datei-Emulation auf zwei Ebenen statt: Untersuchung auf Betriebssystem- und Überwachung des Execute-Flows auf CPU-Ebene. Damit können Angriffe schon auf der Exploit-Ebene abgefangen werden. Denn es gibt tausende Schwachstellen und Millionen verschiedener Malware-Implementierungen, doch es gibt nur sehr wenige Exploits, mittels denen Cyber-Kriminelle Schwachstellen eines Betriebssystems ausnutzen können.



Da E-Mail Protect Pro keine zusätzliche Hardware oder Software benötigt, eignet sich die Lösung hervorragend für Unternehmen, die eine Lösung ohne große Anschaffungskosten (CAPEX), komplexe Installation oder aufwendige Verwaltung suchen. Das Produkt bietet mittels hoher Verfügbarkeit und einem 24/7/365 Managed Service den optimale Schutz vor E-Mail basierten Angriffen für jede Unternehmensgröße.

Funktionsübersicht

TECHNOLOGIE	BESCHREIBUNG
ECHTZEIT-SCHUTZ VOR VIREN, SPAM UND PHISHING-ATTACKEN	Mittels mehrstufiger Filterverfahren, zwei Antivirus-Engines, sowie heuristische Analysen schützen die Echtzeit-Mechanismen vor Spam und Malware. Modernste Methoden wie die SFP (Sender Policy Framework), die Spoofing Protection sowie die Recurrent Pattern Detection wehren proaktiv Spoofing-, Phishing- und DHA- bzw. DOS-Angriffe ab.
QUARANTÄNE	Als Spam erkannte E-Mails werden in der Quarantäne festgehalten. Nutzer erhalten regelmäßig einen Spam-Report, mittels dessen sie entscheiden können, ob die geblockten Spams zugestellt oder gelöscht werden sollen, ohne dass sie sich an der Quarantäne anmelden müssen.
OUTBOUND	Schutz ausgehender E-Mails um zu vermeiden, dass ungewollt Spams oder Viren verschickt werden. Daher wird jede versandte E-Mail untersucht, schadhafte E-Mails geblockt und der Sender informiert.
DRITTER VIRENSCANNER	Erweiterung der im Standard vorhandenen zwei Antiviren-Engines um einen weiteren Antiviren-Scanner für zusätzlichen Schutz.
VIRUS OUTBREAK DETECTION	Unsere Virus Outbreak Detection (kurz VOD) erkennt Viren auf Basis heuristischer Analysen und ist damit die perfekte Ergänzung zu herkömmlichen Anti-Viren Systemen. VOD stoppt E-Mails, die mit hoher Wahrscheinlichkeit einen bis dato unbekannten Virus beinhalten.
APT PROTECT PRO	APT Protect Pro bietet mittels signaturunabhängiger Untersuchungen von Dateien Schutz vor Ransomware und unbekannten Sicherheitslücken. Dabei setzt die Lösung eine zweistufige Sandbox-Emulation auf Betriebssystem- und CPU-Ebene ein, um Malware bereits in der Exploit-Phase zu erkennen.