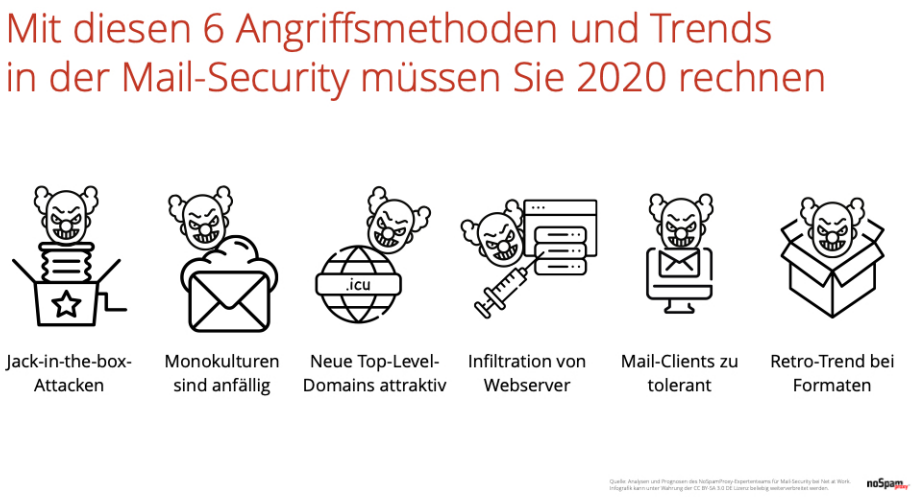
MEDIA ALERT / PRESSEMITTEILUNG

Mit diesen 6 Mail-Attacken müssen Sie 2020 rechnen

Mail-Security-Experten von NoSpamProxy veröffentlichen Prognose zu wichtigsten Malware-Trends und Angriffsmethoden auf Mail-Kommunikation in 2020.

Paderborn, 15. Januar 2020 – Net at Work GmbH, der Hersteller der modularen Secure-Mail-Gateway-Lösung NoSpamProxy aus Paderborn, veröffentlicht eine Prognose zu den sechs bedeutendsten Methoden für Mail-Attacken in 2020. Das NoSpamProxy-Team wertet regelmäßig umfangreiche Datenquellen aus und analysiert kontinuierlich die aktuelle Bedrohungslage. Als Anbieter von Mail-Security-Lösungen ‚Made in Germany' legt NoSpamProxy dabei einen besonderen Fokus auf den deutschsprachigen Raum und seine spezifischen Gegebenheiten.



Mail-Security-Experten von NoSpamProxy benennen Trends für 2020

Nach Auswertung der Daten aus 2019 über Angriffsmethoden und -formen zum Jahresende erwarten die Security-Experten vor allem folgende sechs Trends für 2020:

1. Jack-in-the-box-Attacken mit sich schnell ändernden Links

Die Infrastruktur der Angreifer wird immer ausgefeilter und performanter: Harmlose Links in Mails werden dabei für immer kürzere Zeiten durch bösartige Links ausgetauscht. So sind sie auch für große Prüfnetzwerke immer schwerer zu erkennen bzw. wenn sie erkannt werden, sind die Links bereits wieder gegen harmlose zurückgetauscht worden. Damit wird das Klicken auf selbst auf geprüfte Links zum Nervenkitzel.

2. Monokulturen sind anfällig

Große Mail-Infrastrukturen wie Office 365 und SaaS-Mail-Sicherheitslösungen sind attraktive Angriffsziele und werden in 2020 noch gezielter angegriffen werden. Bereits in 2019 wurden beispielsweise in Office 365 verstärkt entsprechende Angriffe aus infiltrierten E-Mail-Accounts heraus beobachtet.

3. Neue Top-Level-Domains finden reißenden Absatz bei Cyberkriminellen

Die neuen Top-Level-Domains (TLD) wie .icu, .site und .best sind für Angreifer besonders interessant. Mit 14% aller neuen generischen TLDs steht .icu an der Spitze und stellt bereits über 5% der Domains, die Malware verbreiten.

4. Vermehrte Infiltrierung von Webservern

Warum eigene vertrauenswürdige Domains aufbauen, wenn man Malware auf Webservern bereits bekannter Domains platzieren kann? Diesen Ansatz machen sich immer mehr Mail-Attacken zunutze. Die Security-Experten von NoSpamProxy konnten bereits in 2019 zahlreiche solcher Angriffe beobachten, mit stark steigender Tendenz. Von daher wird die Absicherung von Webservern auch in 2020 weiter ein brandaktuelles Thema darstellen und beispielsweise das regelmäßige Patchen von Wordpress-Installationen immer wichtiger.

5. Toleranz von Clients wird missbraucht

Mail-Clients sind äußerst fehlertolerant, damit sie auch Mails anzeigen können, die nicht zu 100% dem RFC entsprechen. Denn obwohl der Aufbau und der Versand von E-Mails durch RFCs genau festgelegt ist, halten sich längst nicht alle E-Mail-Versender an die Vorschriften. Die in bester Absicht in Clients eingebaute Toleranz machen sich Angreifer immer häufiger zunutze, um beispielsweise bekannte Absender vorzutäuschen oder den realen Absender zu verschleiern. Die Experten von Net at Work haben in den letzten Monaten einige neue Varianten davon beobachtet. Für 2020 erwarten die Experten einen Anstieg dieser Angriffe. Eine umfassende Prüfung der Absenderinformation am Gateway ist daher wichtiger denn je.

6. Retro-Look auch bei Archivformaten

Uralt-Archivformate, die kaum noch produktiv eingesetzt werden, werden auf Clients von Packer-Software wie beispielsweise 7zip immer noch erkannt und verarbeitet. Viele der gängigen Viren- und Malwarescanner können diese Formate jedoch nicht mehr analysieren. Es ist zu erwarten, dass alte Archivformate in 2020 die neuen Lieblingsverstecke von Malware werden.

„Wir überwachen und analysieren kontinuierlich die Bedrohungslage in der Mail Security. Mit unseren Auswertungen möchten wir Unternehmen, Verwaltungen und andere Organisationen dafür sensibilisieren, dass die Sicherheit der E-Mail-Kommunikation nur durch stetige Anpassung der Abwehrmaßnahmen erreicht werden kann“, erläutert **Stefan Cink, E-Mail-Sicherheitsexperte bei Net at Work**. *„Auch auf die kommenden Bedrohungen in 2020 kann man sich mit den richtigen Werkzeugen gut vorbereiten. Flexibilität und Automatisierungsgrad sind hier Trumpf.“*

Beispielweise lassen sich Bedrohungen über neue Top-Level-Domains oder durch alte Packer-Formate mit feingranularen Regeln gut abfangen. Selbstlernendes Whitelisting und die detaillierte Auswertung der Senderreputation erlauben hier eine optimale Kombination von Sicherheit, Automatisierung und Praxistauglichkeit – insbesondere auch in SaaS-Umgebungen. *„Letztlich ist es in der Mail-Kommunikation nicht anders als im realen Leben: Die Vertrauenswürdigkeit meines Gegenübers ist entscheidend für meine Reaktion“*, fasst Cink zusammen.

Weitere Informationen über die integrierte Mail-Security-Suite NoSpamProxy erhalten Sie hier:
https://www.nospamproxy.de

Interessenten können NoSpamProxy mit telefonischer Unterstützung kostenlos testen:
https://www.nospamproxy.de/de/produkt/testversion

Zusammenfassung

Mail-Security-Experten von NoSpamProxy veröffentlichen Prognose zu wichtigsten Methoden und Trends bei Angriffen auf die E-Mail-Kommunikation in 2020.

Keywords

2020, Angriffsmethoden, Mail-Attacken, Malware-Trends, Mail Security

Über NoSpamProxy und Net at Work

Net at Work unterstützt als IT-Unternehmen seine Kunden mit Lösungen und Werkzeugen für die digitale Kommunikation und Zusammenarbeit. Der Geschäftsbereich Softwarehaus entwickelt und vermarktet mit NoSpamProxy ein innovatives

MEDIA ALERT / PRESSEMITTEILUNG

Secure E-Mail-Gateway mit erstklassigen Funktionen für Anti-Spam, Anti-Malware und E-Mail-Verschlüsselung, dem weltweit mehr als 4.000 Kunden die Sicherheit ihrer E-Mail-Kommunikation anvertrauen. Die mehrfach ausgezeichnete Lösung – unter anderem Testsieger im unabhängigen techconsult Professional User Ranking – wird als Softwareprodukt und Cloud-Service angeboten. Mehr zum Produkt unter: www.nospamproxy.de

Im Servicegeschäft ist Net at Work als führender Microsoft-Partner mit acht Gold-Kompetenzen erste Wahl, wenn es um die Gestaltung des Arbeitsplatzes der Zukunft auf Basis von Microsoft-Technologien wie Office 365, SharePoint, Exchange, Skype for Business, Teams sowie Microsoft Azure als cloudbasierte Entwicklungsplattform geht. Dabei bietet das Unternehmen die ganze Bandbreite an Unterstützung: von punktueller Beratung über Gesamtverantwortung im Projekt bis hin zum Managed Service für die Kollaborationsinfrastruktur. Über die technische Konzeption und Umsetzung von Lösungen hinaus sorgt das Unternehmen mit praxiserprobtem Change Management dafür, dass das Potential neuer Technologien zur Verbesserung der Zusammenarbeit auch tatsächlich ausgeschöpft wird. Net at Work schafft Akzeptanz bei den Nutzern und sorgt für bessere, sichere und lebendige Kommunikation, mehr und effiziente Zusammenarbeit sowie letztlich für stärkere Agilität und Dynamik im Unternehmen.

Die Kunden von Net at Work finden sich deutschlandweit im gehobenen Mittelstand wie beispielsweise Diebold-Nixdorf, CLAAS, Miele, Lekkerland, SwissLife, Uni Rostock, Würzburger Versorgungs- und Verkehrsbetriebe und Westfalen Weser Energie.

Net at Work wurde 1995 gegründet und beschäftigt derzeit mehr als 100 Mitarbeiter in Paderborn und Berlin. Gründer und Gesellschafter des inhabergeführten Unternehmens sind Uwe Ulbrich als Geschäftsführer und Frank Carius, der mit www.msxfaq.de eine der renommiertesten Websites zu den Themen Office 365, Exchange und Skype for Business betreibt. www.netatwork.de

Unternehmenskontakt

Frau Aysel Nixdorf, Marketing & PR, T +49 5251 304627, aysel.nixdorf(at)netatwork.de
Net at Work GmbH, Am Hoppenhof 32 A, D-33104 Paderborn, www.netatwork.de

Pressekontakt

Team Net at Work, T +49 7721 9461 220, netatwork(at)bloodsugarmagic.com
bloodsugarmagic GmbH & Co. KG, Gerberstr. 63, D-78050 Villingen-Schwenningen, www.bloodsugarmagic.com