MSP
Barracuda
Your journey, secured.

WHITEPAPER

KLICK ICH ODER KLICK ICH NICHT?

Warum E-Mails zum grössten Cybersecurity-Einfallstor und Email-Security zum Must-Have im MSP-Portfolio geworden sind.

2020

INFINIGATE MSP
.... Adding Security to MSP & Cloud

Klick ich oder klick ich nicht?

Warum E-Mails zum grössten Cybersecurity-Einfallstor und Email-Security zum Must-Have im MSP-Portfolio geworden sind.

In diesem Whitepaper erfahren Sie:

- Wie sich E-Mails zur grössten Cybersecurity-Falle entwickelt haben.
- Wie Sie als MSP diese Herausforderungen als Chance nutzen können.
- Welche Email-Bedrohungen sie unbedingt kennen sollten.
- Welche Lösungen und Service-Konzepte es rund um Email-Security für Sie gibt.

Schwachstelle menschliche Firewall

Im Bereich der Cyber-Sicherheit gibt es einen einfachen Grund dafür, dass Emails die Nummer Eins Bedrohung darstellen – und es ist sehr wahrscheinlich, dass sich dies in naher Zukunft nicht ändern wird: Menschen öffnen Emails.

Es braucht lediglich eine Person in der Organisation ein Attachment herunterladen oder einen Link anzuklicken, der auf eine Webseite führt, die mit Schadprogrammen infiziert ist, um die ganze Organisation zu gefährden.

Momentan gibt es unzählige Vorfälle, bei denen Organisationen mit Erpressungstrojanern (= Ransomware) aufgefordert werden, entweder mittels Zahlung an Cyber-Kriminelle den Zugang zu verschlüsselten Daten wiederzuerlangen oder Fälle, bei denen erhebliche Kosten für die Datenwiederherstellung verursacht werden.

Größtenteils wurde die Malware durch einen Email-Anhang verbreitet, der mit Hilfe von Social Engineering Techniken genau dafür hergestellt wurde. Diese sind oft so gut gemacht, dass auch der IT erfahrenste Endverbraucher dazu verleitet wird, den Anhang herunterzuladen.

Email-Attacken weiter im Aufwärtstrend

In 96 Prozent der Cyberangriffe war es eine E-Mail an einen Mitarbeiter, die den Angreifern als Einfallstor diente.[1] Gezielte Email Attacken, die über einen gefährdeten Email Account gesteuert werden, sind nach neuesten Entwicklungen der erfolgreichste Email-Attacken-Überträger.

Trotz all dem stagnieren die Investitionen in E-Mail-Sicherheit, im Bezug auf andere Bereiche, seit Jahren auf einem vergleichsweise niedrigen Niveau. Nach Angaben des Marktforschungsinstituts Gartner entfallen lediglich 8 Prozent des IT-Security-Budgets auf die Absicherung des E-Mail-Kanals.[1]

Covid19 bietet neue Lockfallen

Abgelenkt durch externe Faktoren und ausserordentliche Bedingungen werden die Enduser in dieser Zeit besonders mit Inhalten rund um das Coronavirus zu folgenschweren Handlungen animiert.

Betreffzeilen und Email-Content reichen von WHO-News zur aktuellen Situation bis hin zu Angeboten von raren Produkten wie Atemschutzmasken mit entsprechenden Shops.

Herausforderungen als Chance für MSP

Der Markt für Email-Sicherheit boomt! Eine stetig wachsende Anzahl von Endgeräten, immer neue und unterschiedliche Modelle im Hinblick auf Anschaffung, Miete- oder Nutzungsmodelle, die immer vernetztere Arbeitswelt und vor allem die Nutzung von Cloud-basierten Mailbox-Diensten führen zu immer komplexer werdenden Anforderungen bezüglich E-Mail-Sicherheit.[2]

Vorurteile weichen auf

Die digitale Transformation, die bei vielen KMU seit einigen Jahren ein Fokusthema in den Business-Prozessen darstellt, wird - gewollt oder gezwungen - aktuell durch die Coronakrise nochmals verstärkt vorangetrieben. Vorurteile wurden aufgeweicht und Kritiker mussten umdenken, um sich in neue Arbeitswelten zu begeben. Umso grösser ist heute das allgemeine Erstaunen über die Möglichkeiten und die Flexibilität, die diese neuen Arbeitswelten mit sich bringen.

Rückschritte sollen vermieden werden

Mit den neuen Arbeitsweisen rücken auch die Möglichkeiten für neue Business Modelle in den Fokus der Entscheidungsträger. Einen Rückschritt nach der Pandemie möchte niemand machen und diese Chance gilt es nun für MSP zu nutzen. Insbesondere kleinen und mittelständischen Unternehmen fehlt es sowohl an Ressourcen als auch an Kenntnissen, um allen Anforderungen dieser neuen digitaleren und somit auch ein gutes Stück komplexeren Arbeitswelt gerecht zu werden.

Umfassende Service-Portfolios sind die Zukunft

Die Einnahmen im cloudbasierten Email-Sicherheitsmarkt werden voraussichtlich spätestens im Jahr 2023 ein Volumen von 1.1 Milliarden USD erreicht haben, und somit unter dem Strich eine jährliche Wachstumsrate von 7.8 Prozent verzeichnen. Dabei wird ein Großteil dieser Einnahmen durch diejenigen Managed Service Provider (MSP) erreicht werden, welche die notwendige Erfahrung für ein herausragendes Email-Security Angebot mitbringen.[3]

3 gute Gründe für Email Security im MSP-Modell

1 Mehr Sicherheit durch aktuelle Applikationen

Malware und perfide Attacken unterbrechen immer wieder den Arbeitsalltag und machen es zunehmend schwerer, Daten und Prozesse nachhaltig abzusichern. Der Schutz von lokal installierter Lizenzsoftware verliert mit der Entwicklung der Hackerangriffe schleichend seine Wirkung, bis einzelne oder mehrere Bereiche ausgeliefert sind.

Mit Managed Email profitieren die Kunden von laufend aktuellen Features und Technologien, um jederzeit auf neueste Bredrohungsszenarien reagieren zu können. Sie, als Managed Service Provider, können Ihr Angebot laufend optimieren und dem Kunden somit den wirksamsten Schutz gewährleisten.

2 Managed Email Security spart dem Kunden Zeit & Kosten

Mit der Integration von Email-Security in Ihr MSP-Portfolio sparen Sie Ihren Kunden Zeit, Aufwand und Nerven für die stetige Betreuung der Email-Systeme. Ausserdem profitieren die Kunden mit MSP-Modellen von vergleichsweise geringen regelmässigen und kalkulierbaren Kosten, im Gegensatz zu hohen Initialinvestitionen für Ausstattung und Infrastruktur. Vollkommen problemlos lassen sich die MSP-Modelle skalieren und der jeweiligen Situation anpassen.

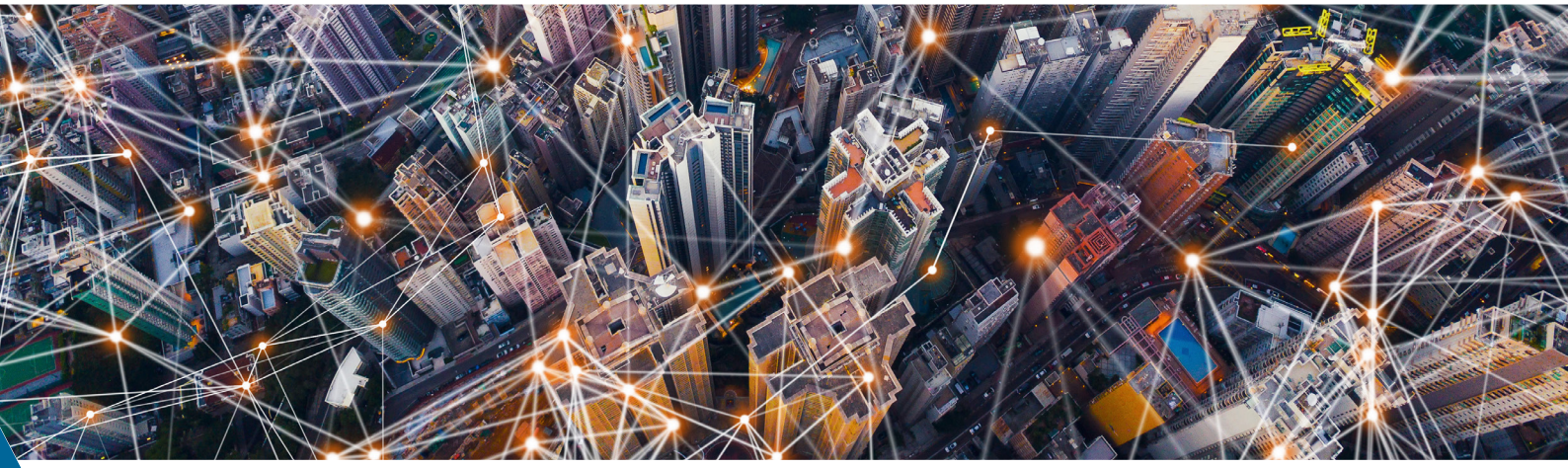
3 Fachkompetenz vom Spezialisten

Mit Ihnen als IT-Partner wissen Ihre Kunden den Datenverkehr, ob Ein- oder Ausgang, in guten Händen. Gerade für sensible Unternehmensbereiche sind DIY-Lösungen kein guter Ratgeber. Nebst Zeit- und Kostengründen ist es wichtig, Unternehmenskorrespondenzen stetig zu sichern. Wer bleibt da ständig auf dem neuesten Stand, wer betreibt den Aufwand, sich 24/7 mit diesen Themen zu beschäftigen? Sie, als Partner und Lösungsanbieter.

Der Kampf gegen Email-Angriffe wird immer komplexer

In der heutigen, sich schnell entwickelnden Umgebung reichen traditionelle E-Mail-Security-Lösungen nicht mehr aus, um Unternehmen zu schützen. Unternehmen müssen sich wirksam gegen ausgeklügelte E-Mail-Bedrohungen wehren können, die Standard-Abwehrmechanismen durch den Einsatz von Hintertürtechniken einfach umgehen. Mittels Spoofing, Social Engineering und Betrug werden ganze Netzwerke durchdrungen und grosse Schäden angerichtet.

Während E-Mail-Gateways eine solide Grundlage darstellen, verringert eine durchgehend angewendete, mehrschichtige Schutzstrategie die Anfälligkeit für E-Mail-Angriffe und trägt zu einer besseren Verteidigung des Unternehmens, sowie der Daten und Mitarbeiter bei.



13 Email-Bedrohungen, die Sie kennen sollten

1. Spam

Hierbei handelt es sich um unerbetene, hochvolumige Nachrichten kommerzieller Art, die ohne Rücksicht auf die Identität des Empfängers versendet werden.

2. Malware

Als Maleware wird Software bezeichnet, die speziell entwickelt wurde, um Schäden an technischen Anlagen anzurichten, Betriebsunterbrechungen herbeizuführen, Daten zu exfiltrieren oder auf andere Weise Zugang zu einem entfernten System zu erhalten. Malware wird üblicherweise mittels E-Mail-Anhängen oder URLs, die zu Websites mit infiziertem Inhalt leiten, versendet.

3. Daten-Exfiltration

Diese Arten von Angriffe treten auf, wenn Daten, ohne Zustimmung des Eigentümers, von einem entfernten System kopiert oder abgerufen werden. Sie kann böswillig oder versehentlich erfolgen.

4. URL-Phishing

Bei Phishing-Angriffen versuchen Cyberkriminelle für böswillige Zwecke an sensible Informationen, wie Benutzernamen, Passwörter oder Bankdaten zu gelangen. Beim URL-Phishing verwenden Cyberkriminelle E-Mails, um ihre Opfer zur Eingabe sensibler Informationen auf einer gefälschten Website, die wie eine legitime Website aussieht, zu bewegen.

5.Scamming

Beim Scamming nutzen Cyberkriminelle betrügerische Konstrukte, um das Opfer zur Preisgabe persönlicher Informationen zu verleiten. Beispiele für Scamming sind gefälschte Stellenausschreibungen, Investitionsmöglichkeiten, Erbschaftsmitteilungen, Lotteriegewinne und Geldüberweisungen.

6. Spear Phishing

Spear-Phishing ist eine hoch personalisierte Form des E-Mail-Phishing-Angriffs. Cyberkriminelle definieren ihre Ziele detailliert und entwerfen sorgfältig konzipierte Botschaften, wobei sie sich oft als vertrauenswürdige Kollegen, Website oder Unternehmen ausgeben.

Spear-Phishing-E-Mails versuchen in der Regel, sensible Informationen zu stehlen, wie z.B. Login-Ausweise oder finanzielle Details, die dann für Betrug, Identitätsdiebstahl und andere Straftaten verwendet werden. Cyberkriminelle machen sich bei ihren Spear-Phishing-Angriffen auch sozial-technische Taktiken zunutze, einschließlich Dringlichkeit, Kürze und Druck, um die Erfolgswahrscheinlichkeit zu erhöhen.

7. Domain Impersonation

Bei der Domain Impersonation oder Domain-Imitation versuchen Angreifer sich als eine gewisse Domain auszugeben, indem sie Techniken wie Typosquatting verwenden, einen oder mehrere Buchstaben in einer legitimen E-Mail-Domain durch einen ähnlichen Buchstaben ersetzen oder einer legitimen E-Mail-Domain eine schwer zu erkennende kleine Änderung hinzufügen.

8. Markenimitationen

Markenimitationen sollen ein Unternehmen oder eine Marke imitieren, um ihre Opfer zu täuschen, damit sie antworten und persönliche oder anderweitig sensible Informationen preisgeben.

9. Blackmail

Erpresserische Betrugsmails und Sextortionangriffe nehmen in hoher Frequenz zu, werden ausgefeilter und umgehen immer häufiger E-Mail-Gateways. Bei Sextorsionsangriffen nutzen Cyberkriminelle gestohlene Benutzernamen und Passwörter, nehmen unter Verwendung dieser Informationen mit den Opfern Kontakt auf und versuchen, sie dazu zu bringen, ihnen Geld zu geben. Die Betrüger behaupten beispielsweise, ein auf dem Computer des Opfers aufgezeichnetes kompromittierendes Video zu haben und drohen, dieses an alle Kontakte des Opfers weiterzugeben - es sei denn das Opfer zahlt.

10. Business Email Compromise

Bei BEC-Angriffen geben sich die Betrüger als Mitarbeiter der jeweiligen Organisation aus, um das Unternehmen selbst, seine Mitarbeiter, Kunden oder Partner zu betrügen. In den meisten Fällen konzentrieren die Angreifer ihre Bemühungen auf die Mitarbeiter, die Zugang zu den Finanzen oder sensiblen Informationen des Unternehmens haben, wobei Einzelpersonen getäuscht werden, Überweisungen zu tätigen oder sensible Informationen offen zu legen. Diese Angriffe verwenden Social-Engineering-Taktiken und enthalten oft keine Anhänge oder Links.

11. Conversation Hijacking

Bei Gesprächsübernahmen, sog. Conversation Hijacking, klinken sich Cyberkriminelle in bestehende Geschäftsgespräche ein oder leiten neue Gespräche auf Grundlage der ihnen vorliegenden Informationen ein, die sie vorher aus gehackten E-Mail-Konten gesammelt haben, um Geld oder persönliche Informationen zu stehlen.

Angreifer verbringen hier viel Zeit mit dem Durchlesen von E-Mails und der Überwachung des gehackten Kontos, um das Geschäft zu verstehen und Details über Operationen, laufende Geschäfte, Zahlungen und Verfahren zu erfahren.

12. Lateral Phishing

Beim lateralen Phishing nutzen Angreifer kürzlich gekaperte Konten, um Phishing-E-Mails an ahnungslose Empfänger zu versenden, wie etwa enge Kontakte im Unternehmen und Partner bei externen Organisationen, um den Angriff zu verbreiten. Da diese Angriffe von einem legitimen E-Mail Konto und einem vertrauenswürdigen Kollegen zu stammen scheinen, haben sie in der Regel eine hohe Erfolgsquote.

13. Kontoübernahme

Die Kontoübernahme ist eine Form von Identitätsdiebstahl und Betrug, bei der eine böswillige dritte Partei erfolgreich Zugriff auf die Zugangsdaten eines Benutzers erhält. Cyberkriminelle verwenden Markenimitationen, social Engineering und Phishing, um Anmeldeinformationen zu stehlen und auf E-Mail-Konten zuzugreifen. Sobald das Konto gehackt wird, überwachen und verfolgen die Hacker die Aktivitäten, um zu erfahren, wie das Unternehmen Geschäfte macht, die E-Mail-Signaturen, die sie verwenden, und die Art und Weise, wie finanzielle Transaktionen abgewickelt werden.

Dies hilft ihnen bei erfolgreichen Angriffen und Sammeln zusätzlicher Anmeldeinformationen für andere Konten.

Steigern Sie die Produktivität von kleineren und mittleren Unternehmen (KMU)

Unternehmen jeglicher Größe benötigen eine einfach zu verwaltende und umfassende Produktivitätslösung. Sie müssen sich vor E-Mailbasierten Angriffen schützen. Darüber hinaus benötigen sie Möglichkeiten zur Archivierung von E-Mails mit richtlinienbasierter Aufbewahrung, Suchfunktionen sowie automatisierte Backup- und Wiederherstellungsfunktionen für E-Mails, Anhänge und Dateien.

Barracuda Essentials for Office 365 – MSP bietet Sicherheit und Schutz für Office 365-Umgebungen

Dreifachschutz durch mehrstufige Email Security, Compliance-Archivierung und Cloud-to-Cloud Backup-Funktionen

Dadurch profitieren Ihre Kunden von einer schnelleren, sichereren und effizienteren Vorbereitung, Migration und Ausführung. Mit Barracuda Essentials for Office 365 – MSP können Sie Ihren Kunden das beruhigende Gefühl geben, dass ihre E-Mail-, Daten- und Cloud-Infrastruktur vollständig geschützt ist.

ESS
MSP
Barracuda
Essentials

Barracuda Essentials for Office 365 – MSP

Professionelle MSP-Lösung

- Cloud-basierte Lösung für Email Security mit Verschlüsselung und Schutz vor Datenverlusten (Data Loss Prevention, DLP)
- Cloud-basierte Archivierung für Compliance- und eDiscovery-Zwecke
- PST-Management zur schnelleren Migration
- Schutz vor dem versehentlichen oder böswilligen Löschen von E-Mails und Daten

Automatisierte und bedarfsgesteuerte Backups

Mit den Cloud-to-Cloud-Backup-Lösungen von Barracuda für Microsoft Office 365-Umgebungen schützen Sie Ihre Exchange Online-Postfächer sowie One-Drive for Business- und SharePoint Online-Dateien und -Ordner vor Datenverlusten und unbeabsichtigtem Löschen.

Barracuda Essentials for Office 365

Schutz vor E-Mail-Bedrohungen

Barracuda Email Security Service umfasst Advanced Threat Protection, um von E-Mails ausgehende Angriffe von den Netzwerken Ihrer Kunden fernzuhalten. Außerdem sorgt die Lösung für einen unterbrechungsfreien E-Mail-Verkehr und schützt das Netzwerk vor Datenlecks.

Archivierung zu Compliance-Zwecken

Barracuda Cloud Email Archiving Service wird in Office 365 integriert, um ein Cloud-basiertes, indiziertes Archiv zu erstellen. Sie können dadurch detaillierte Aufbewahrungsrichtlinien erstellen, umfangreiche Suchvorgänge und Audits durchführen, Berechtigungen festlegen, gesetzliche Aufbewahrungspflichten erzwingen und E-Mails exportieren.

Ganzheitliche Security-Konzepte sind die Zukunft

Wenn ein MSP seinen Secure Mail Service startet, ist der Schritt zu einem umfangreicheren Service nur noch klein: Mit Hilfe einer breiten Angebotspalette von tagtäglich neuen Cybersecurity Technologien können auch die Firewalls und Endpoint Software leicht verwaltet werden.

MSPs sind außerdem in der einzigartigen Position, intelligente Security Applikationen aufzusetzen, die proaktiv die Thread Prevention unterstützen. Angesichts der Tatsache, dass die Komplexität der Attacken im Cybersecurity-Umfeld deutlich zunimmt, sollten MSPs sich vor Augen halten, dass sich Malware heutzutage nicht nur in den Systemen der Kunden befindet, sondern sich auch gerne in den Applikationen selbst verbergen oder umgekehrt.

Sogenannte Threat Hunting Technologien machen es deutlich einfacher, Malware proaktiv zu lokalisieren.

Training as a Service

Einer der am meisten unterschätzen Aspekte für Provider im MSP Bereich sind persönliche Trainings. Bei den End Usern muss erst einmal ein gewisses Know-How-Level aufgebaut werden, damit sie Malware überhaupt erkennen können.

Auf den Punkt gebracht bedeutet das, dass es mit jedem nicht heruntergeladenen Stück Malware einen Vorfall weniger gibt, bei dem ein MSP eingreifen muss. Das spart Zeit und Kosten und stärkt das Vertrauen in den MSP.

Für welchen Service im Bereich Cybersecurity sich ein MSP auch immer entscheidet – alle Mangend Services sollten im Bereich Email Protection gestartet werden.

Email-Kommunikation ist das am häufigsten genutzte Einfallstor für alle Malware und somit der am stärksten gefährdete Bereich einer IT-Infrastruktur.

1. https://www.computerworld.ch/security/firmenbeitraege/im-cyberkrieg-oberhand-behalten-2146425.html, 4.5.2020
2. https://computerwelt.at/news/markt-fuer-e-mail-sicherheit-boomt/, 4.5.2020
3. Cloud-Based Email Security Market, Orbis Research, February 2018.

Kontaktieren Sie uns für ein Live-Webinar oder Beratungsgespräch.

Gerne beraten wir Sie persönlich zu Ihren Möglichkeiten.

Mario Becker
Partner Development Manager MSP
Tel.: +49 157 35992801
mbecker@barracuda.com

Franziska Lillge
Field Marketing Manager MSP (DACH)
Tel.: +49 171 2424 698
flillge@barracuda.com