HORNETSECURITY

INFOPAPER

CYBERKRIMINELLE IM VORWEIHNACHTSGESCHÄFT – 5 TIPPS WIE SIE IHR UNTERNEHMEN AM BESTEN SCHÜTZEN

Das Jahr neigt sich dem Ende: es wird kälter, früher dunkel und die ersten machen sich verzweifelt Gedanken, was sie ihren Liebsten wohl zu Weihnachten schenken sollen. Die Onlineshop-Anbieter und lokalen Geschäfte stellen sich auf das alljährliche und umsatzstarke Vorweihnachtsgeschäft ein.

Den Startschuss gibt die Rabattschlacht am letzten Novemberwochenende mit dem **Black Friday und Cyber Monday.** Ideal daher auch für Unternehmen zu diesen Tagen entsprechende Angebote für ihre Kunden zu platzieren, um die inneren Schnäppchenjäger herauszulocken. Doch nicht nur für Unternehmen ist dieses Geschäft äußerst lukrativ, auch Cyberkriminelle möchten einen ordentlichen Weihnachtsbonus kassieren.
Welche Angriffsarten werden am häufigsten von Cyberkriminellen genutzt? Was macht die Attacken so gefährlich? Und wie verändert die Corona Pandemie das Vorweihnachtsgeschäft? Das und mehr erläutern wir im folgenden Infopaper und geben Ihnen **5 Tipps wie Sie Ihr Unternehmen am besten schützen.**

Inhalt

Vorsicht: Cyberkriminelle in Weihnachtsstimmung...oder doch nicht?

Cyberkriminelle Banden nutzen für ihre Attacken aktuelle und medienwirksame Ereignisse.

Dies dürfte jedem spätestens seit Aufkommen des Coronavirus klargeworden sein: Vermehrte Hackerangriffe auf medizinische Einrichtungen, Attacken auf Forschungslabore sowie Phishing-Angriffe mit Bezug auf gefälschte Corona-Tests oder Rabattaktionen für Mund-Nasen-Masken schmückten bereits die Schlagzeilen.

Einen entsprechenden Anstieg an Cyberattacken per E-Mail verzeichnete das Hornetsecurity Security Lab seit Februar 2020, wie folgende Grafik zeigt:

ABB. 1: Anstieg an Spam, Infomail and Malware vor und während Corona

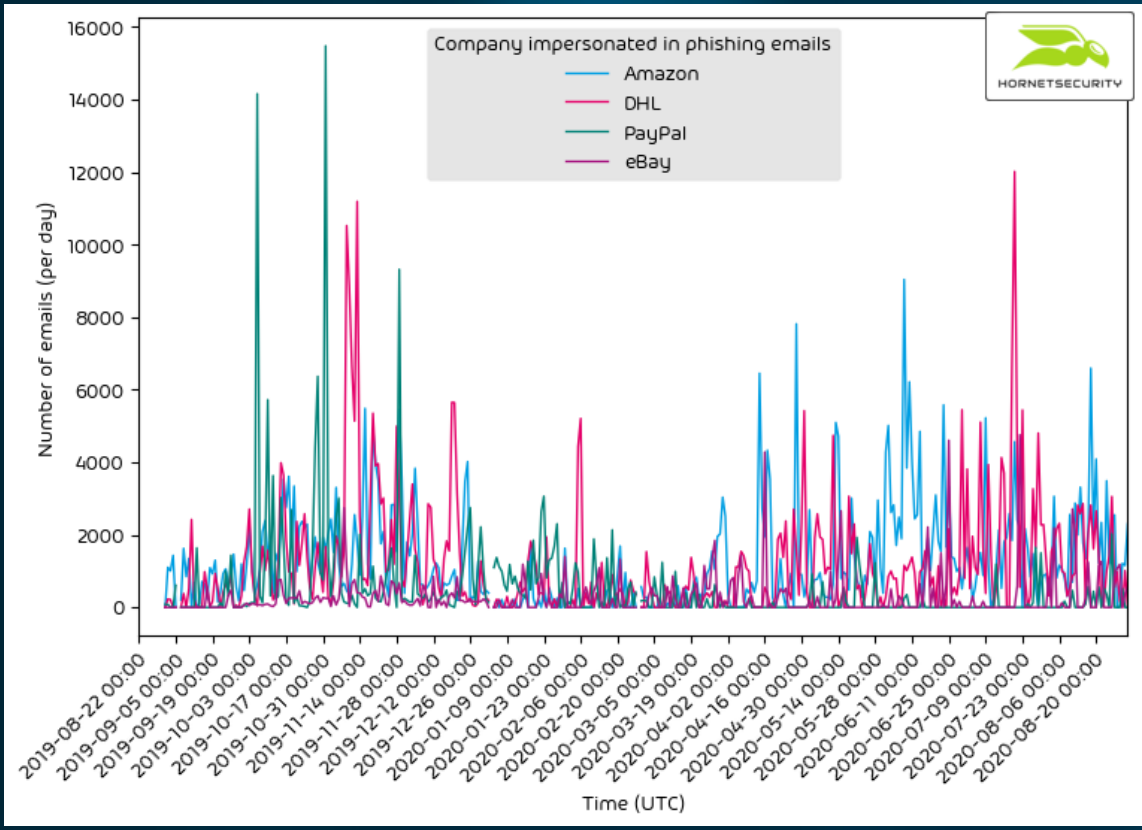
Obwohl die Corona-Pandemie noch längst nicht vorbei ist, steht bereits ein weiteres Ereignis an, welches auch die vergangenen Jahre immer wieder als **Aufhänger für Cyberattacken genutzt wird: Das Vorweihnachtsgeschäft rund um den Black Friday und Cyber Monday.**

Doch wie sieht der Konsumbedarf in Zeiten von Corona eigentlich aus? Sind nach wie vor Black Friday und Cyber Monday wichtig, um Schnäppchen zu machen? Die Antwort ist: Ja.

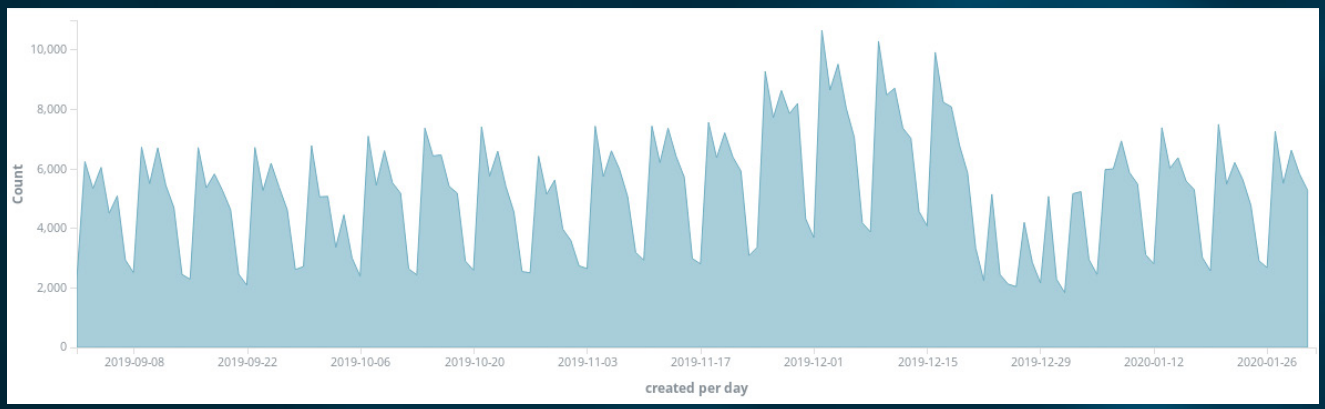
Google startete Mitte des Jahres bereits eine weltweite Umfrage an seine Nutzer, um herauszufinden, wie die Corona Pandemie das Kaufverhalten ändert. **75% der befragten Nutzer planen ihr Online-Weihnachtsshopping in diesem Jahr sogar zu verstärken.** Wo die letzten Jahre immer noch einige Konsumenten lieber lokal in Geschäften einkauften, verschiebt sich alles zunehmend ins Internet. Somit rechnen die Internet-Shop-Anbieter in diesem Jahr mit einer steigenden Nachfrage, aber auch mit erhöhtem Konkurrenzdruck. Besonders dann, wenn der stationäre Handel sich ebenfalls im Online-Geschäft bewährt und der Preis besonders im Fokus steht. Durch die Kurzarbeit und vermehrte Arbeitslosigkeit weltweit, gehen Online-Anbieter in den Preiskampf und Konsumenten auf Schnäppchenjagd.

All dies bedeutet gleichzeitig mehr Angriffsfläche für Cyberkriminelle.

Vergangenes Jahr beobachtete das Security Lab von Hornetsecurity einen **Anstieg an Phishing-Kampagnen von November bis Mitte Dezember.** Die gefälschten E-Mails locken oft mit verführerischen Angeboten zur Vorweihnachtszeit und den konsumstarken Tagen wie Black Friday und Cyber Monday.



Vor allem der Online-Riese Amazon muss mit seiner populären Marke immer wieder für die kriminellen Aktivitäten von Hackern herhalten. **Ab Ende November wurden im Namen von Amazon vermehrt Phishing-E-Mails versendet.**
Dies zeigt folgende Beobachtung des Hornetsecurity Security Labs aus dem letzten Jahr:



Doch nicht nur mit Phishing-Angriffen sind dieser Tage vermehrt zu rechnen, vor allem Online-Händler müssen sich auf einen **Anstieg an DDoS-Angriffen** einstellen. Mit einer Flut an Server-Anfragen zwingen Hacker die Systeme der Anbieter in die Knie, wodurch viele Verkaufschancen vertan werden.

Aber damit nicht genug: **Bereits seit zwei Jahren infolge meldet sich Emotet mit weihnachtlichen Grüßen zum Ende des Jahres zurück.** Es ist daher nicht unwahrscheinlich, dass auch in diesem Dezember mit einem **erhöhten Aufkommen an Ransomware-Angriffen auf Unternehmen zu rechnen ist.**

Im Folgenden geben wir Ihnen einen umfassenden Einblick in die Bedrohungssituation, die sich durch DDoS-, Phishing- und Ransomware-Angriffen ergibt. Abschließend sollen Ihnen 5 hilfreiche Tipps dabei helfen sich vor der **zunehmenden Professionalisierung dieser Angriffsarten** zu schützen.

„Server down." Wie DDoS-Attacken Online-Händler in die Knie zwingen

Für die digitale Geschäftswelt stellen sie eine der größten Bedrohungen überhaupt dar: DDoS-Attacken. **Sie können bei den betroffenen Unternehmen einen enormen wirtschaftlichen Schaden verursachen und nicht zuletzt enorm am Image kratzen.**

Eine DDoS-Attacke steht als Abkürzung für Distributed Denial of Service-Attacken. Im Gegensatz zur DoS-Attacke werden hier mehrere zuvor gekaperte Systeme dazu benutzt, gegen das Zielsystem vorzugehen. **Der Angriff besteht darin, an einen Server übermäßig viele Anfragen zu stellen, sodass das Zielsystem überlastet wird** und auf weitere Anfragen nicht mehr reagieren kann.

Zielsysteme sind beispielsweise ein Mailserver oder Webserver eines Unternehmens. Gerade in der Vorweihnachtszeit ist ein solcher Ausfall, wenn auch nur für kurze Zeit, fatal. Alle von dem Server abhängigen Dienste sind nicht mehr oder nur eingeschränkt abrufbar. Der Kundenstamm schwappt über zur Konkurrenz und der Internetshop-Anbieter verbringt die Weihnachtszeit mit Reparaturarbeiten.

Opfer von DDoS-Angriffen waren bereits kleine Shops, doch auch große bekannte Online-Händler wie Amazon und Otto sind vor solchen Attacken nicht gefeit. **Besonders zu besonderen Ereignissen, geht von DDoS-Angriffen eine erhöhte Gefahr aus.**

So konnte das BSI in seinem Lagebericht etwa feststellen, dass **zum Vorweihnachtsgeschäft sowie zum Black Friday und Cyber Monday vermehrt derartige Angriffe** gestartet werden.

Das professionelle Geschäft mit DDoS-Attacken

Neben der zunehmenden Professionalisierung von Phishing Angriffen, entwickeln sich auch DDoS-Attacken kontinuierlich weiter. Dazu zählen beispielsweise **technisch elaborierte Angriffe, die anstatt bandbreitenstarke nun zunehmend ausgefeilte Strategien nutzen.**

Das BSI verzeichnete im vergangenen Jahr einen Anstieg an Meldungen über aktiv gesteuerte Angriffe, bei denen Angreifer auf die Sicherheitsabwehr des Zielservers reagierten und den Angriff damit deutlich verstärkten.

In der zweiten Jahreshälfte in 2019 stellten Analysten darüber hinaus die **Anwendung des sogenannten Carpet Bombing** fest. Bei dieser Angriffsstrategie umgehen Angreifer die klassischen Schutzmaßnahmen an der Netzwerkgrenze, sodass sie sich unter den Detektions-Schwellenwerten (in Gbit/s) befinden und so nicht vom System erkannt werden.

Dazu richten die Hacker ihren Angriff gegen eine große Anzahl an IP-Adressen innerhalb des Netzwerks.

Unternehmen stehen damit neuen und professionalisierten DDoS-Strategien gegen, wobei auch klassische Schutzlösungen an ihre Grenzen stoßen. Um solche fortschrittlichen Angriffe abzuwehren sind dynamische Gegenmaßnahmen erforderlich.

Das zahlt sich aus: Wie Hacker mit Ransomware-Attacken profitieren

Ransomware, auch Verschlüsselungs- und Erpressungstrojaner genannt, ist ein Schadprogramm, welches dafür sorgt, dass Dateien für den Benutzer gesperrt und nur gegen ein Lösegeld wieder freigeschaltet werden. **Haupteinfallstor bildet die geschäftsrelevante E-Mail-Kommunikation.**

Eine Ransomware wird in der Regel durch andere Schadprogramme, welche hinter Anhängen oder URLS verborgen sind, nachgeladen. Öffnet der Nutzer die schädliche Datei oder den Link, ist die erste Hürde überwunden und die Ransomware gelangt auf den Computer. Sobald die Schadsoftware aktiv wird, beginnt die Verschlüsselung der Dateien. Dabei können einzelne Dateien auf einem System oder sogar mehrere Systeme innerhalb eines Unternehmensnetzwerkes verschlüsselt werden. Um wieder Zugriff auf die Dateien zu erlangen, soll das Opfer ein Lösegeld zahlen.
Doch es gibt keine Garantie dafür, nach einer Bezahlung die Dateien tatsächlich zurückzuerhalten.

Die Schäden für Unternehmen sind bei einer erfolgreichen Ransomware-Attacke enorm. So konnten Angreifer im Jahr 2018 allein in den USA insgesamt 8 Milliarden Dollar erbeuten. Im Jahr 2019 sogar knapp 24 Milliarden Dollar.

Der entstandene Schaden bei den betroffenen Unternehmen ist in der Regel weitaus größer als ein gegebenenfalls gezahltes Lösegeld. So entstehen erhebliche Mehrkosten durch die Bereinigung und Wiederherstellung von Systemen. Bei vielen Unternehmen zieht ein erfolgreicher Ransomware-Angriff darüber hinaus einen Reputationsverlust nach sich.

Gerade in der umsatzstarken Vorweihnachtszeit ist mit einem erhöhten Aufkommen an Angriffen mit Ransomware zu rechnen. Um den Betriebsablauf zu erhalten, ist die Chance größer, dass Unternehmen ein Lösegeld zahlen – diese Tatsache wird von den Cyberkriminellen gnadenlos ausgenutzt.

Neue Strategien bei Ransomware-Attacken

Das bloße Verschlüsseln von Dateien scheint mittlerweile längst nicht genug für Cyberkriminelle zu sein. Seit 2019 wurde eine neue Strategie bei cyberkriminellen Banden beobachtet.
So drohten beispielsweise die Akteure hinter der Maze Ransomware mit einer Veröffentlichung von gestohlenen Dateien, wenn die Lösegeldzahlung des betroffenen Unternehmens ausbleibt. Diese Masche verleiht Ransomware-Attacken eine neue Gefahrendimension. **Das betroffene Unternehmen befindet sich damit noch mehr im Zugzwang, um die sensiblen Daten vor einer Veröffentlichung zu schützen.**
Internetshop-Anbieter etwa speichern neben persönlichen Angaben ihrer Kunden, wie Namen und Adresse auch oftmals sensible Zahlungsinformationen, die höchst schutzbedürftig sind. Bei Veröffentlichung dieser Daten käme an dieser Stelle ein immenser Reputations- sowie Umsatzverlust zum Tragen.

Vorsicht Abzocke: Phishing-Attacken auf Weihnachtsmission

Wie bereits zu Anfang dargestellt, sind Phishing-E-Mails eine häufige und einfache, aber dennoch sehr effektive Angriffsart. Angreifer versuchen sich mithilfe von Phishing Zugriff auf sensible und persönliche Daten zu verschaffen. Dazu **nutzen die Angreifer die schwer kontrollierbare Schwachstelle aus: den Menschen**.
Sie appellieren in der Regel an Eigenschaften wie Hilfsbereitschaft, Angst, Dringlichkeitsempfinden oder Respekt vor Autoritäten, und versuchen so ihre Opfer zu manipulieren.

Dabei orientieren sie sich verstärkt an aktuellen Ereignissen wie Rabatt-Aktionen zum Black Friday. Hier ist ein besonders wachsames Auge bei der Bearbeitung von E-Mails gefragt, gerade im diesjährigen Vorweihnachtsgeschäft, wo auch mit mehr Rabattaktionen zu rechnen ist.

Professionalisierung von Phishing-Mails

Der nigerianische Prinz hat längst ausgedient: Phishing-Angriffe werden **zunehmend professionalisiert und lassen sich dadurch nur schwerlich von Originalen unterscheiden.** So sind grammatikalische und orthografische Mängel nur noch selten anzufinden, stattdessen sind Phishing-Mails häufiger in grammatikalisch korrekter Sprache verfasst. Auch der Einsatz von HTTPS-Protokollen macht das Entlarven von Phishing-Angriffen nicht einfacher:

In seinem Lagebericht der IT-Sicherheit 2020 erläutert das BSI, dass **Cyberkriminelle vermehrt HTTPS-Links in Phishing-Nachrichten nutzen**. Lag der Anteil im November 2019 noch bei 44%, so konnte der Dezember mit seinem Vorweihnachtsgeschäft einen Anstieg um 20% verzeichnen.
Die erste Jahreshälfte 2020 verzeichnet ebenso eine stärkere Nutzung von HTTPS-Protokollen in durchschnittlich 75% der Phishing-E-Mails.

Was muss ich als Unternehmen beachten?

Grundsätzlich gilt es sich über das ganze Jahr hinweg um die Sicherheit der internen Unternehmensinfrastruktur zu bemühen. Sicherlich ist dies nicht immer hoch priorisiert, weil IT-Security bei den meisten Unternehmen nicht zum Kerngeschäft gehört.

Gerade dann sind **Full-Managed-Services genau das Richtige.**
Wir empfehlen mit Blick auf die oben beschriebene Gefährdungslage die folgenden fünf Schutzmaßnahmen:

- **Schutz vor Spam und Malware:** Eine erste Sicherheitsbarriere ist geschaffen, wenn die E-Mail-Kommunikation vor Spam und Malware-Attacken geschützt wird.
- **Schutz vor Phishing:** Zudem sollte ein Hauptaugenmerk auf Phishing-Angriffe gelegt werden. Besonders in Nachrichten eingebettete Links sollten im Fokus stehen. Mit URL-Scanning werden Verlinkungen in E-Mails untersucht und in einer gesicherten Umgebung geöffnet. Sobald der Link vom System als verdächtig eingestuft wird, erhält der Nutzer eine Benachrichtigung.
- **SChutz vor DDoS-Attacken:** Entsprechende Sicherheitslösungen sollten hier in der Lage sein, frühzeitig den Schwung an Anfragen abzublocken. Im Hinblick auf die Nutzung von Carpet Bombing sollte im Notfall eine Ausfallsicherung implementiert werden, die bei einer Störung des Servers unterbrechungsfrei einspringen kann.
- **Schutz vor Ransomware-Attacken:** Klassische Anti-Viren-Filter stoßen bei der ausgefeilten Angriffstaktik an ihre Grenzen. Entsprechende Sicherheitslösungen sollten mindestens eine Sandbox nutzen, um verdächtige Anhänge in einer sicheren Umgebung zu öffnen und das auch mit entsprechendem Zeitversatz. Nicht selten werden die schädlichen Funktionen einer Ransomware erst zu einem späteren Zeitpunkt aktiviert. Einige Anbieter, wie Hornetsecurity, bieten zudem intelligente Erkennungsmechanismen an, die in der Lage sind, gezielte Angriffe auf besonders gefährdete Personen zu entlarven und auf bestimme Inhaltsmuster, die auf bösartige Absichten schließen lassen, zu reagieren.

Als verantwortungsvoller Online-Shop-Betreiber sollten Sie auch auf den Schutz Ihrer Kundschaft bedacht sein:

- ☑ Geben Sie Ihren Kunden Hinweise über aktuelle Phishing-Kampagnen.
- ☑ Richten Sie eine Hotline für jegliche Verdachtsfälle ein, die Ihre Kunden melden können.
- ☑ Geben Sie ihren Kunden Informationen an die Hand wie sie Ihre Nachrichten von Phishing-Nachrichten unterscheiden können.

Als cloudbasierter E-Mail-Security-Anbieter hat Hornetsecurity ganzheitliche E-Mails-Sicherheits-Services im Portfolio. Mit Advanced Threat Protection sichern Sie Ihren E-Mail-Verkehr vor Phishing-, Ransomware und Targeted Attacks ab. Sie nutzen Microsoft 365? In Sekundenschnelle lässt sich die 365 Total Protection Suite in ihr Microsoft 365 nahtlos integrieren und schützt Sie mit 21 Features ganzheitlich vor Cyberattacken per E-Mail.

www.hornetsecurity.com