HORNETSECURITY

CYBERTHREAT REPORT
1ST EDITION 2020

In Zeiten, in denen informationstechnische Systeme nicht mehr nur isoliert eingesetzt werden, sondern global über Internet und Mobilfunk vernetzt sind, steigt auch die Bedrohung durch Cyberattacken. Illegale Aktivitäten im Internet reichen von Betrugsversuchen, Phishing und DDos-Angriffen bis hin zum Verkauf von Schwarzmarktware, wie Drogen und Waffen. Laut dem Bundeskriminalamt gibt es in kaum einem anderen Deliktsbereich einen so kontinuierlichen Anstieg krimineller Aktivitäten.[1]

Der Cyberraum verändert sich schnell – und so auch die Methoden, die Hacker und Betrüger nutzen. Weshalb Cyberkriminalität zu den globalen Bedrohungen gehört, welche Rolle Künstliche Intelligenz in Zukunft bei Cyberattacken und dessen Abwehr spielen wird und warum Hacker Microsoft Office 365 vermehrt ins Visier nehmen, thematisiert die 1st Edition des Hornetsecurity Cyberthreat Report 2020.

Cybercrime: Ein globales Risiko

Der Global Risk Report 2019 zeigt, dass Cyberangriffe nun zum dritten Jahr in Folge neben Wetterextremen, dem Scheitern des Klimaschutzes und Naturkatastrophen zu den schwerwiegendsten globalen Bedrohungen zählen. Großflächige Cyberattacken und der dadurch verursachte **Zusammenbruch Kritischer Infrastrukturen aufgrund eines Cyberangriffs werden sogar als zweithäufigste Gefahr** eingeordnet. Die Sorge um Cyberattacken auf Versorgungsbetriebe (Kritische Infrastrukturen) wächst, denn die Folgen eines längeren Ausfalls sind enorm und nahezu mit den Auswirkungen von Wetterextremen gleichzusetzen.[2]

Cybersicherheit nimmt einen immer größer werdenden Stellenwert bei Sicherheitsfragen in Unternehmen ein. So sehen ganze 92 Prozent der Befragten einer Cybersecurity Studie vom TÜV in Cyberangriffen eine ernstzunehmende Gefahr.[3]

Global Threat Report: Platz 1 bis 3 auf der Liste der globalen Risiken 2019

1 Wetterextreme & Scheitern des Klimaschutzes

2 **Großflächige Cyberangriffe und der darauffolgende Zusammenbruch Kritischer Infrastrukturen**

3 Massenarbeitslosigkeit und andere negative Konsequenzen durch den technischen Fortschritt

Die Integration von Technik in nahezu jeden Bestandteil des menschlichen Lebens eröffnet nicht nur neue Möglichkeiten, sondern bietet zahllose, noch nicht klar definierbare Einfallstore für kriminelle Machenschaften. Neue Technologien werden eingeführt – schneller, als die Sicherheit dieser überprüft und garantiert werden kann.

Spam: Schadhafte Anhänge und Spionage

Es gibt unterschiedliche Arten von Spam, unter anderem den klassischen Spam, bei dem der Empfänger beispielsweise zu einer Vorabüberweisung für eine Dienstleistung oder ein Produkt animiert werden soll. Eine weitere Form ist der Schadprogramm-Spam. Mit Schadprogrammen im Anhang oder durch einen Link in der E-Mail versuchen Cyberkriminelle die Systeme des Empfängers zu infizieren. Die dritte Form ist das Phishing – hier soll der Nutzer Zugangsdaten zum Beispiel für Online-Banking oder Social Media Accounts eingeben.[4]

Die Experten vom Hornetsecurity Security Lab haben die Spam-E-Mails von Oktober 2018 bis Oktober 2019 analysiert und konnten feststellen, dass es sich bei **91,7 Prozent um klassischen Spam** handelte. Die restlichen **8,3 Prozent waren schadhafte Spam-E-Mails (schadhafte Anhänge, URLs oder Phishing).**

Abb. 1: Top 5 der schadhaften Anhänge

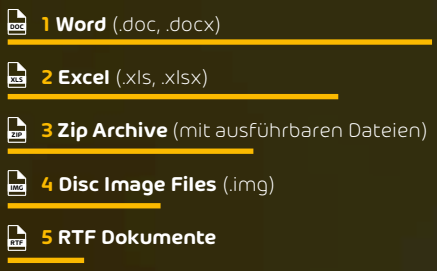


Abb. 2: Anteile der eingegangenen Spam-E-Mails %

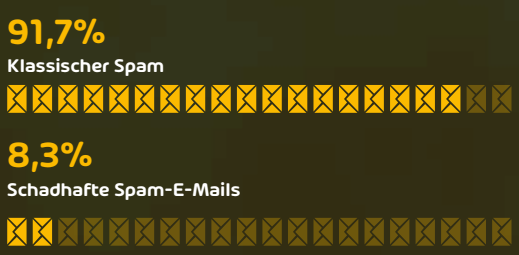


Abb. 3:
Verteilung der Bedrohungsarten in schadhaften Spam-E-Mails

Abb. 4:
Herkunft der Spam-E-Mails

Abb. 5:
Anteil der Malware in schadhaften E-Mails

Mehr als die Hälfte der schadhaften Spam-E-Mails enthält Spyware, Trojaner und Keylogger. Hacker nutzen diese vermehrt, um Spionage zu betreiben und Informationen für einen weiteren Cyberangriff zu sammeln.[5] Zwar ist die Gesamtanzahl an Spam-E-Mails zurückgegangen, jedoch sollte die Gefahr, die von Spam ausgeht, nicht unterschätzt werden. Der steigende Aufwand, den Cyberkriminelle investieren, und die vermehrte Nutzung von persönlichen Daten aus Datenlecks steigern das Risiko einer Infektion erheblich.[6]

Social Engineering: Menschliche Schwäche als Basis für Cyberattacken

Social Engineering bildet schon seit Langem die Grundlage für Betrugsmaschen jeglicher Art. Doch vor allem in den Zeiten der Digitalisierung eröffnet diese perfide Form der Manipulation für Cyberkriminelle Tore. Unternehmen fallen Cyberkriminellen **fast dreimal häufiger durch Social Engineering Attacken** als durch tatsächliche Schwachstellen in ihrer IT-Sicherheitsarchitektur zum Opfer. [7]

Cyberkriminelle nutzen nicht nur gefälschte Absender-E-Mail-Adressen, Fake-Anzeigen und -Websites. Sie platzieren auch sensible Botschaften in ihren Nachrichten. 2019 wurde zum Beispiel die Unsicherheit bezüglich der Datenschutzgrundverordnung als Aufmacher für etliche gefälschte E-Mails benutzt.

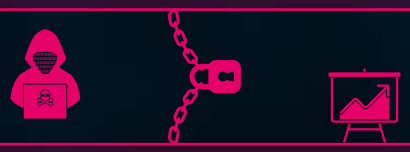
Ransomware: Schäden in Millionenhöhe

Ryuk, GandCrab und Locky sind zurück – und zwar gefährlicher denn je. Sogar das Federal Bureau of Investigation (FBI) warnte im Oktober 2019 vor Ransomware-Angriffen, die Unternehmen und Organisationen in den USA bedrohen. Eine Meldung dieser Art gab es zuletzt 2016, einige Monate vor der Angriffswelle mit WannaCry und NotPetya.[8] Ransomware zählt eindeutig zu den größten Bedrohungen in der Cyberwelt, da Angriffe immer wieder zu **Komplettausfällen von ganzen Rechnernetzwerken und Produktionsanlagen führen.**[9] Laut einer Studie von KPMG waren **60 Prozent der Befragten in den vergangenen zwei Jahren Ziel eines Ransomware-Angriffs.** Bei jedem fünften Unternehmen waren nach einem erfolgreichen Angriff mit Ransomware sogar ganze 75 Prozent der IT-Landschaft betroffen.[10]

Im dritten Quartal 2019 konnte der Versicherer Beazley einen **Anstieg von Angriffen mit Ransomware von rund 37 Prozent** im Vergleich zu den vorangegangenen drei Monaten festgestellt werden.[11]

Cyberkriminelle wittern mit Ransomware nach wie vor lukrative Geschäfte. Das illustriert auch Ryuk: Die gezielte Beobachtung der verwendeten Bitcoin-Adressen lassen laut BSI Rückschlüsse auf ein Lösegeld von **600.000 US-Dollar schließen.** Für Hacker ist Ransomware heutzutage ein etabliertes Geschäftsmodell, das sich stetig weiterentwickelt: GandCrab hat beispielsweise eine Versionsnummer und wird außerdem als Ransomware-as-a-Service, also als Dienstleistung im Internet angeboten.[12]

60% der befragten Unternehmen in Deutschland waren Ziel einer Ransomware-Attacke



+37% Anstieg von Ransomware-Angriffen im Q3 2019

Emotet: Die gefährlichste Schadsoftware der Welt?

Fällt der Name Ransomware, wird oft im selben Zuge auch Emotet genannt. Nicht nur in der deutschen Wirtschaft, auch bei Behörden und Organisationen verursachte Emotet im vergangenen Jahr erhebliche Schäden. Im September 2019 meldete das BSI **mehrere tausend kompromittierte E-Mail-Konten** an die zuständigen Provider.[13]

Doch was macht Emotet so gefährlich? Die Schadsoftware hat sich seit ihrem ersten Auftritt in 2014 als äußerst wandelbar gezeigt. Die erste Version von Emotet wurde durch Links oder über Anhänge in Spam-Kampagnen mit gefälschten Mitteilungen von Banken verbreitet. Später wurde Emotet auch über als Rechnung getarnte PDFs sowie als gefälschte Versandbestätigungen von Amazon in Umlauf gebracht.[14, 15] Insbesondere das sogenannte **„Outlook-Harvesting", die inhaltliche Analyse der E-Mail-Kommunikation** auf einem infizierten Gerät, spielt bei der Erkennung von Emotet eine entscheidende Rolle. Die Schadsoftware liest nicht nur Kontaktbeziehungen aus dem Verlauf, sondern auch die Inhalte der E-Mails aus. Cyberkriminelle können ihre Social Engineering-Techniken somit perfektionieren und noch präzisere, zielgerichtetere E-Mails verschicken.[16]

Mittlerweile verhält sich Emotet wie ein Dropper und lädt nach einer erfolgreichen Infektion weitere Schadprogramme nach: Derzeit beispielsweise den Banking-Trojaner Trickbot, der sich unter anderem über das Auslesen von Zugangsdaten eigenständig in Netzwerken ausbreiten kann. Danach folgt oftmals die Ransomware Ryuk, die ganze Systeme verschlüsseln kann.[17]

Abb. 6: Erweiterungen und Gefahren von Emotet

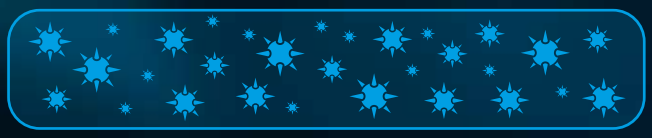
- Outlook-Harvesting
- Diebstahl von Daten aus Webbrowsern
- Nachladen von Schadsoftware, Ransomware
- Ausnutzung nicht gepatchter Schwachstellen
- Weiterverbreitung in lokalen Netzwerken

Bereits in 2018 bezeichnete das BSI **Emotet als gefährlichste Schadsoftware der Welt. Auch in 2019 bleibt dieser Ruf eindeutig unverändert.**

Destructive Malware: Die Zerstörungswut der Hacker

Malware-Attacken mit zerstörerischen Elementen werden bei Cyberkriminellen immer beliebter. Laut einer Studie von IBM hat sich die **Anzahl an Angriffen dieser Art weltweit in der zweiten Jahreshälfte von 2019 verdoppelt.**[18] Seit August 2019 verschlüsselt beispielsweise die **Ransomware GermanWiper** bei der Aktivierung nicht nur die Daten auf den betroffenen Rechnern, sondern überschreibt sie mit Nullen. Obwohl die Entwickler von GermanWiper bei ihren Angriffen Lösegeld von den Opfern fordern, gibt es keine Möglichkeit die verschlüsselten Daten wiederherzustellen. Auch die **Ransomware RobinHood** enthält zerstörerische Elemente und verursachte bereits große Schäden in Baltimore (USA), indem nicht nur die Dateien auf den Rechnern der User verschlüsselt, sondern auch die Backup- und Service-Funktionen behindert wurden.[19]

2019: Angriffe im ersten Halbjahr



2019: Angriffe im zweiten Halbjahr **(+116%)**

Zerstörerische Angriffe kosten multinationale Unternehmen durchschnittlich rund **239 Millionen Dollar** – im Vergleich dazu kosten Datenlecks 3,92 Millionen Dollar im Durchschnitt. Laut IBM brauchen Unternehmen rund **512 Stunden**, um sich von einer Attacke mit zerstörerischer Malware zu erholen und eine einzelne Attacke kann im Durchschnitt **12.000 Geräte pro Unternehmen** beschädigen.[20]

Abb. 7: Durchschnittliche Schäden, die Malware mit zerstörerischen Elementen anrichten kann

512 Stunden	239 Millionen Dollar	12.000 Geräte
...brauchen Unternehmen, um sich von einer Attacke mit zerstörerischer Malware zu erholen.	...kostet ein Angriff mit zerstörerischer Malware.	...werden bei einem Angriff pro Unternehmen geschädigt.

Die steigende Anzahl an Cyberattacken mit zerstörerischer Malware ist besorgniserregend. Die Schäden, die Cyberkriminelle mit dieser Angriffsform verursachen können, sind immens und selbst, wenn das Lösegeld für verschlüsselte Informationen nicht gezahlt wird, kann es zu langfristigen Störungen der Betriebsabläufe und damit einhergehenden großen monetären Verlusten kommen.

Phishing: Noch immer eine Bedrohung

Die Experten vom Hornetsecurity Security Lab konnten im Durchschnitt rund **12,3 Prozent aller eingegangenen E-Mails als Phishing-Angriffe** identifizieren. Trotz des Rückgangs im Sommer steigt die Anzahl der Phishing-E-Mails zum Ende des Jahres wieder, da sich Hacker besonders zur Weihnachtszeit und dem damit einhergehenden Anstieg der Nutzung von Online-Shops wie Amazon höhere Erfolgsquoten versprechen.[21]

In **2018 haben 51 Prozent der britischen Organisationen Maßnahmen für mehr Cybersicherheit ergriffen, 2019 waren es 57 Prozent.**[22] Trotz des Anstiegs des Bewusstseins für die Gefahren, die von Phishing-E-Mails ausgehen, besteht weiterhin ein hohes Risiko für Nutzer.

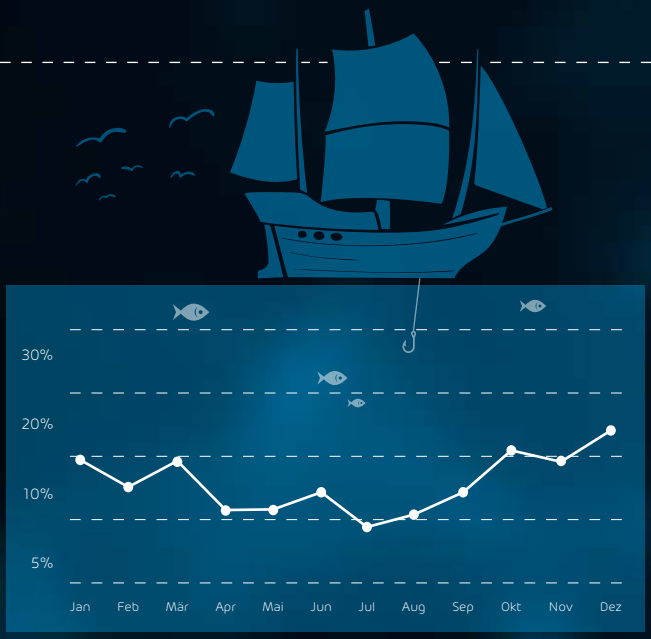


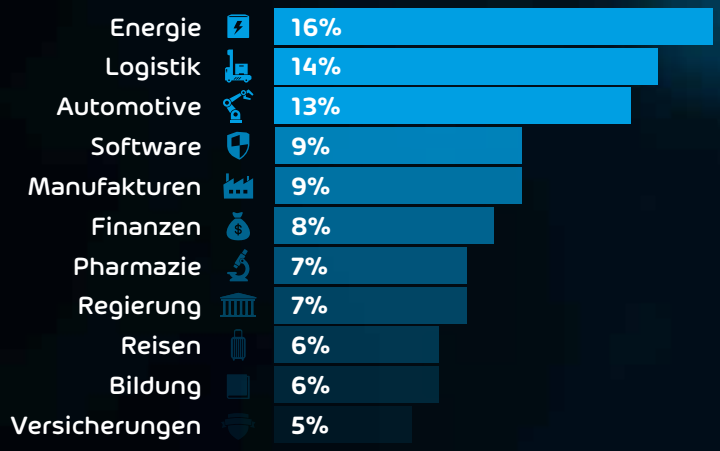
Abb. 8: Entwicklung des Phishing-Anteils von allen eingegangenen E-Mails in 2019[24]

Hacker bedienen sich vermehrt aktueller Themen, um ihre Phishing-E-Mails möglichst echt aussehen zu lassen. Wie bereits im Kapitel zum Thema Social Engineering genannt, wurde im vergangenen Jahr unter anderem die Unsicherheit vieler Nutzer bezüglich der Datenschutzgrundverordnung als Basis für authentische Phishing-E-Mails missbraucht und auch andere, sensible Themen wie aktuelle Naturkatastrophen dienten vermehrt als Basis für Phishing-Angriffe.

Bedrohte Branchen: Energie- und Logistiksektor besonders gefährdet

Das Hornetsecurity Security Lab hat die Top 1000 Domains mit dem größten E-Mail-Volumen analysiert und nach Branchen kategorisiert. Dabei konnten unsere Experten ein eindeutiges Ergebnis ermitteln: **Energieversorger führen die Liste der 10 am häufigsten angegriffenen Branchen mit 16 Prozent an.** Die Logistikbranche folgt mit 14 Prozent, der Automobilsektor mit 13 Prozent. Doch auch Softwareunternehmen, die Pharmaindustrie und die Finanzbranche wurden im Jahr 2019 vermehrt zum Angriffsziel von Hackern.

Abb 9: Top 10 der angegriffenen Branchen in 2019



Die Energieversorgung zählt zu den Kritischen Infrastrukturen, genauso wie Einzelbereiche der Logistikbranche, wie zum Beispiel Lebensmitteltransporte. In beiden Sektoren haben die Betriebsabläufe einen Einfluss auf das Allgemeinwohl der Gesellschaft. Ein Cyberangriff mit Ransomware übt großen Druck auf die Betreiber aus. Die Wahrscheinlichkeit, dass das Geld für die Entschlüsselung gezahlt wird, ist hier ggf. höher als bei anderen Betrieben.

Es ist auch denkbar, dass Angriffe auf diese Bereiche vielfach politisch motiviert sind. Die Installation einer Backdoor im System einer Kritischen Infrastruktur könnten beispielsweise staatliche Hacker im Fall einer Krise als Druckmittel nutzen.

Abb 10: Angriffsarten auf die **Energiebranche**

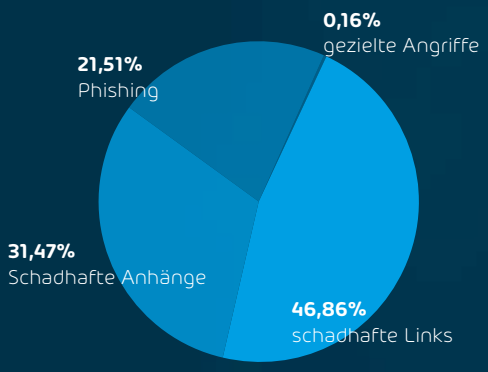


Abb 11: Angriffsarten auf die **Logistikbranche**

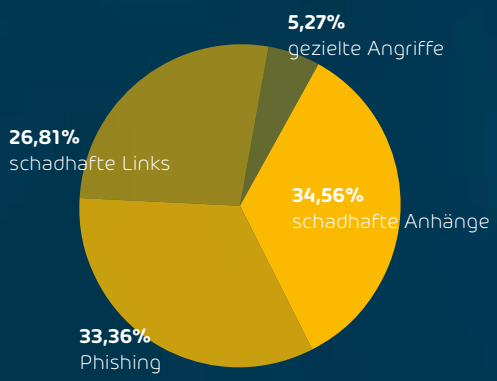
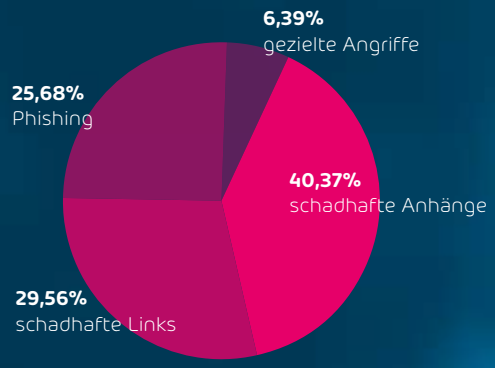


Abb 12: Angriffsarten auf die **Automotive-Branche**



Fast die Hälfte der Angriffe auf Energiebetriebe erfolgte durch E-Mails mit schadhaften Links. Dieser Trend ist darauf zurückzuführen, dass viele Anti-Spam-Lösungen Viren im Anhang bereits erkennen können. E-Mails mit schadhaften Anhängen bleiben jedoch nach wie vor ein üblicher Infektionsweg. Knapp 20 Prozent der Angriffe konnten als Phishing-E-Mails, nur 0,16 Prozent als gezielte Attacken identifiziert werden.

In der Logistikbranche und im Automobilsektor konnte das Hornetsecurity Security Lab vor allem schadhafte Anhänge als beliebte Angriffsmethode der Cyberkriminellen ausmachen. Aber auch Phishing-Kampagnen eignen sich besonders in großen Konzernen dazu, interne Informationen zu sammeln. Die Informationen können für die Industriespionage, aber auch für weitere Cyberangriffe genutzt werden, wie zum Beispiel Spear-Phishing.

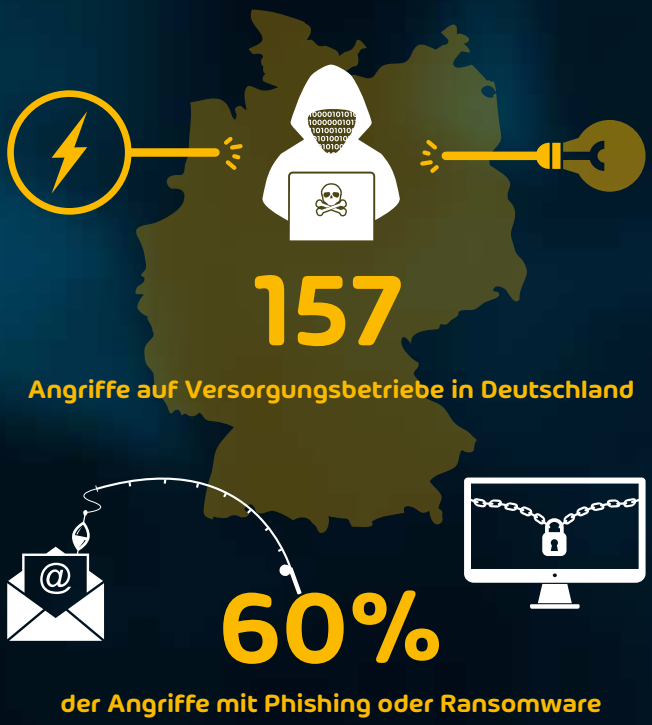
Auch gezielte Angriffe, wie CEO-Fraud, werden von Hackern genutzt, um einzelne Mitarbeiter mittels Social Engineering zu Überweisungen von großen Beträgen zu animieren oder um Industriespionage zu betreiben. **Je nach Branche unterscheiden sich die Angriffsmethoden der einzelnen Hacker, doch vor allem ihre Motive spielen eine entscheidende Rolle.**

Besonders im Bereich Kritischer Infrastrukturen ist anzunehmen, dass der Treiber cyberkrimineller Aktivitäten nicht ausschließlich das große Geld ist. Versorgungsbetriebe gelten als schützenswert, was strenge Auflagen der Regierung zur Sicherheit der Systeme beweisen. Im nachfolgenden Kapitel wird das Thema Kritische Infrastrukturen noch einmal genauer beleuchtet.

Wenn der Strom nicht mehr fließt: Angriffe auf Kritische Infrastrukturen

In der zweiten Jahreshälfte von 2018 kam es laut dem BSI zu rund 157 IT-Sicherheitsvorfällen – 2017 waren es im ganzen Jahr nur 145.[25] Auch in 2019 bleibt die Gefährdungslage beständig auf hohem Niveau, wie die Analyse des Security Labs im vorigen Kapitel zeigt. Während Cyberkriminelle lediglich eine Schwachstelle ausfindig machen müssen, stehen Betreiber Kritischer Infrastrukturen vor der Herausforderung, ihre Systeme vollumfassend und ganzheitlich zu schützen.[26]

Auch in einer Studie des Bundesministeriums für Bildung und Forschung zum Thema **IT-Sicherheit Kritischer Infrastrukturen** gaben mehr als die Hälfte der Befragten an, im letzten Jahr Opfer von Cyberangriffen geworden zu sein. Das Angriffsspektrum ist vielfältig: im Zusammenhang mit Kritischen Infrastrukturen wurde vor allem der Einsatz von Phishing und Ransomware genannt. **60 Prozent der Befragten gaben an, von Cyberattacken dieser Art betroffen gewesen zu sein.**[27]

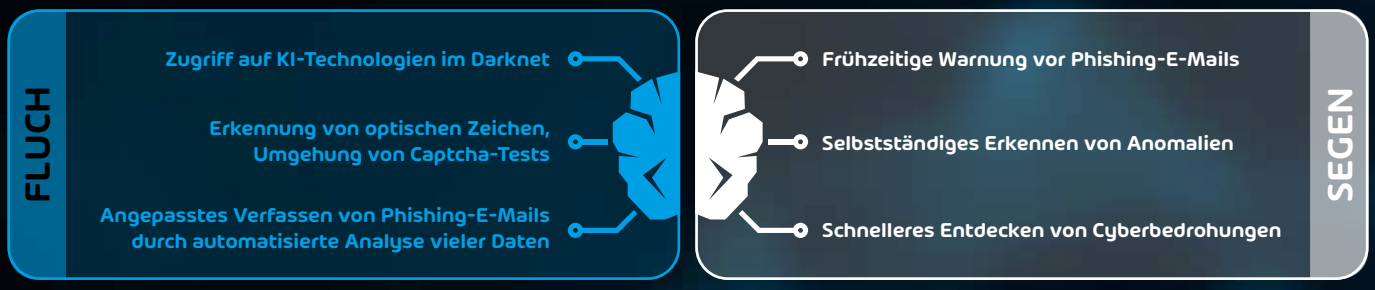


Wie im vorangegangenen Kapitel zu lesen, kamen auch die Experten vom Hornetsecurity Security Lab zu ähnlichen Erkenntnissen: Die Energiebranche ist die am häufigsten angegriffene Branche seit Anfang 2019. Ein Großteil der Angriffe erfolgte durch E-Mails, die schadhafte Links oder Anhänge enthalten, rund 20 Prozent der Angriffe waren Phishing-Attacken. Bereits ein einzelner erfolgreicher Angriff auf einen Versorgungsbetrieb kann schwere Folgen für das alltägliche Leben haben – deshalb verdient die Cybersicherheit Kritischer Infrastrukturen besondere Aufmerksamkeit.

Künstliche Intelligenz: Fluch oder Segen?

KI-Technologien entwickeln sich weiter – und so auch die Komplexität der Cyberangriffe mit Künstlicher Intelligenz als Hilfsmittel, denn das Angebot von KI im Darknet wächst. Mit dem leichten Zugriff auf die Technologien steigt auch das Risiko, dass Hacker sich diese zu Nutze machen.

Herkömmliche Sicherheitstechniken, wie zum Beispiel Captcha-Tests, können bereits mit KI-Software umgangen werden, die fähig sind, optische Zeichen zu erkennen und zu bewerten.[28] Cyberkriminelle können Künstliche Intelligenz außerdem zur Analyse von Nutzerdaten verwenden, um zum Beispiel **Phishing-E-Mails noch glaubwürdiger aussehen zu lassen.** Durch die zunehmende Automatisierung durch KI wird auch die Anzahl an Angriffen steigen, was IT-Verantwortliche vor eine weitere große Herausforderung stellen wird.[29]



Doch Unternehmen können Cyberkriminelle mit ihren eigenen Waffen bekämpfen. **72 Prozent der Unternehmensentscheider glauben, dass KI die Cybersicherheit bei Routine-Aufgaben unterstützen kann.** So können Künstliche Intelligenzen beispielsweise frühzeitig vor Phishing-E-Mails warnen und selbstständig Anomalien erkennen, indem Metadaten automatisch analysiert werden. Auch die Anzahl von False-Positive-Meldungen kann durch KI verringert werden, denn sie kann große Datenmengen präzise und schnell auswerten.[30, 31]

Auch die Verweildauer, in der Viren, Malware und Ransomware unentdeckt bleiben, ist mit dem Einsatz von KI um 11 Prozent gesunken.[32] Künstliche Intelligenzen werden künftig eine große Rolle im Bereich der Cybersicherheit spielen, ob bei cyberkriminellen Angriffen oder zur Verteidigung.

Microsoft Office 365: Des Hackers liebstes Kind

Das Auslagern von IT-Infrastrukturen wird vor allem bei Unternehmen und Organisationen immer beliebter. Bereits 2017 nutzten zwei Drittel die Cloud, jede fünfte Organisation plante die Implementierung. **In Zukunft wird voraussichtlich ein Großteil des Datenverkehrs über die Cloud laufen.** Die Office 365 Cloud von Microsoft gehört zu den beliebtesten Services dieser Art, zwischen 2015 und 2017 ist die Zahl der Abonnenten um **320 Prozent gestiegen**.[33]

Rund 100 Millionen Business-Kunden nutzen die Microsoft Office 365 Suite – sensible Daten, Unternehmensgeheimnisse und personenbezogene Informationen werden dort ausgetauscht und verwahrt. Doch die hohen Nutzerzahlen locken auch Cyberkriminelle an. So konnte bereits 2018 ein beachtlicher Anstieg an Angriffen ermittelt werden. Laut Recorded Future schmückte Microsoft ganze acht Plätze auf der Top Ten Liste der am meisten ausgenutzten Schwachstellen – **sechs dieser Schwachstellen in Office-Anwendungen**.[34] Microsoft selbst meldete einen **Anstieg von Angriffen um 250 Prozent.**[35]

Die Top 6 der Sicherheitslücken befinden sich in Office Anwendungen

Wie verwundbar ist die MS Office Cloud?

In der Cloud **entfallen von Unternehmen gesteuerte Schutzmechanismen, wie die Firewall.** Um Zugang zu einer Vielzahl an Daten zu bekommen, müssen Cyberkriminelle nur eine einzige Schwachstelle im System finden. Mit unterschiedlichen Methoden der Verschleierung schummeln Cyberkriminelle E-Mails in das Postfach der Nutzer und greifen im Ernstfall die Login-Daten eines Office-Accounts ab.

Bereits ein einziger kompromittierter Account in der Datenwolke bietet Cyberkriminellen eine Plattform für viele weitere Angriffe.[36] Von hier aus können Hacker andere Nutzer beispielsweise mit Business E-Mail Compromise zum Überweisen hoher Geldbeträge animieren oder Spionage betreiben.

Business E-Mail Compromise: Globale Verluste

Die finanziellen Schäden, die durch Business E-Mail Compromise verursacht werden, sind immens. Das FBI konnte herausfinden, dass es zwischen Juni 2016 und Juli 2019 zu 166.349 Vorfällen in den USA kam, die mehr als 26 Milliarden Dollar Verluste verursacht haben. Werden die durchschnittlichen Erträge, die Kriminelle bei einem Bankraub erbeuten, mit den Erträgen, die durch Business E-Mail Compromise erwirtschaftet werden, verglichen, erübrigt sich die Frage nach dem Grund der steigenden Cybercrime-Rate.

Bankraub: **$ 3.000**
Business E-Mail Compromise: **$ 130.000**

Laut FBI zielen Cyberkriminelle mit Business E-Mail Compromise Angriffen auf jeden ab, der Geld hat, doch vor allem große Unternehmen und Organisationen, die mit höheren Geldsummen arbeiten, fallen den Hackern zum Opfer.[37]

Durch die hohen Nutzerzahlen hat sich die Microsoft Office 365 Cloud zu einem attraktiven Ziel für Cyberkriminelle entwickelt. Unternehmen wird geraten Lösungen von Drittanbietern nutzen, um sich umfassend zu schützen. Zusätzliche Authentifikationsmechanismen verhindern unauthorisierte Logins, die Verschlüsselung der Daten in der Cloud bietet Sicherheit vor unbefugter Einsicht durch Dritte.

Ausblick

Die Bedrohung durch Cyberkriminalität wächst, ein Abwärtstrend ist in nächster Zeit nicht zu erwarten. Emotet ist nach neuesten Erkenntnissen des BSI noch immer die gefährlichste Schadsoftware der Welt und Ransomware gilt allgemein als größte Bedrohung für Unternehmen und Organisationen. Trotz zunehmender Cyber Security Awareness stellen auch Phishing-E-Mails weiterhin eine große Gefahr dar, weil Cyberkriminelle ihre Betrugstechniken immer weiter perfektionieren, um so selbst geschulte Nutzer zu überlisten.

Auch Kritische Infrastrukturen sind zunehmend gefährdet. Cyberattacken auf Versorgungsbetriebe können **eine Bedrohung der nationalen Sicherheit** darstellen. Denn ein Angriff auf das Energienetz oder die Wasserversorgung kann massive Versorgungsengpässe verursachen.

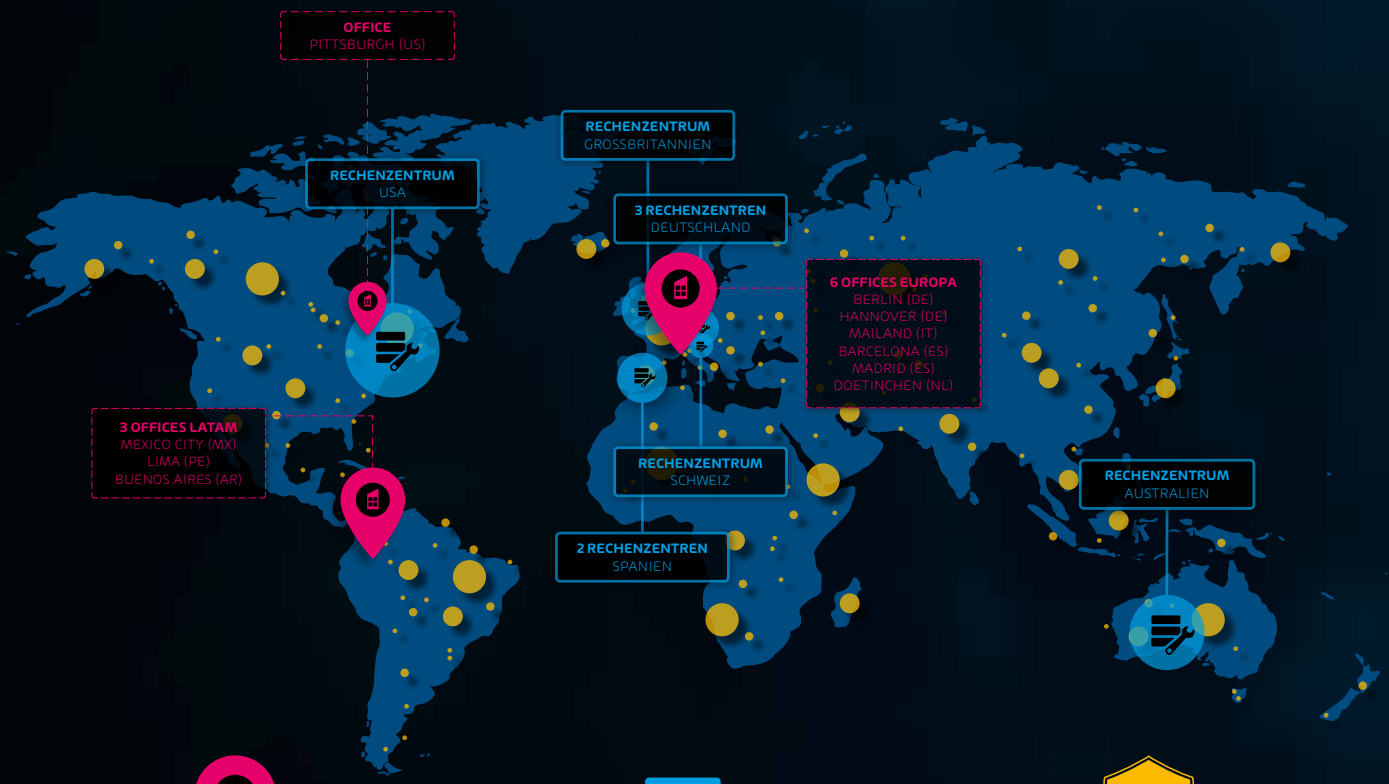
Schlussendlich lässt sich sagen: Auch Cyberkriminelle gehen mit dem technologischen Fortschritt. Die Angriffsmuster werden komplexer, multivektorale Angriffe sind keine Rarität mehr. Für Unternehmen wird es schwieriger, sich gegen derartige Angriffe zu wappnen. **Die E-Mail stellt noch immer den Haupteinfallsvektor für einen Großteil der Cyberangriffe dar.** Besonders Nutzer der Office 365 Suite sind von Cyberangriffen über das Einfallstor E-Mail gefährdet. Im ihrem Fall ist die Sicherung der E-Mail-Kommunikation auf allen Ebenen durch Sicherheitslösungen von Drittanbietern essenziell.

Cyberangriffe sollten genauso wie andere Straftaten ernstgenommen werden. Neben dem Diebstahl sensibler Daten von Privatpersonen sind auch die finanziellen und Reputationsschäden einer Organisation durch Cyberattacken immens. Nicht umsonst haben Regierungen aus aller Welt Allianzen gebildet oder Ämter geschaffen, die die Bevölkerung über Cyberkriminalität und deren Auswirkungen informieren und schützen sollen.

Über Hornetsecurity

Hornetsecurity ist der in Europa führende deutsche Cloud Security Provider für E-Mail und schützt die IT-Infrastruktur, digitale Kommunikation sowie Daten von Unternehmen und Organisationen jeglicher Größenordnung. Seine Dienste erbringt der IT-Sicherheitsspezialist aus Hannover über weltweit neun redundant gesicherte Rechenzentren. Das Produktportfolio umfasst Lösungen in den Bereichen E-Mail-, Web- und File-Security. Alle Services des Unternehmens sind in kurzer Zeit implementierbar und rund um die Uhr verfügbar. Hornetsecurity ist mit rund 200 Mitarbeitern global an zehn Standorten vertreten. Zu den Kunden zählen unter anderem Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA und Claas.

Hornetsecurity international



10 OFFICE STANDORTE
WELTWEIT, DAVON 6 IN EUROPA

9 RECHENZENTREN
WELTWEIT, DAVON 3 IN DEUTSCHLAND

40.000 UNTERNEHMEN
VON UNS GESCHÜTZT

Quellen

(1) https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html

(2) http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

(3) https://www.vdtuev.de/dok_view?oid=769635

(4) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

(5) Spam-Statistik Security Lab, Jan 2019 bis September 2019

(6) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=6

(7) https://www.securitymagazine.com/articles/88907-verizon-2018-data-breach-investigations-report-ransomware-still-a-top-cybersecurity-threat

(8) https://www.it-daily.net/shortnews/22517-neue-ransomware-warnung-des-fbi-was-sie-wissen-muessen

(9) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

(10) https://klardenker.kpmg.de/der-erpresser-aus-dem-internet/

(11) https://www.beazley.com/news/2019/beazley_breach_insights_october_2019.html

(12) https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf;jsessionid=22BBCB1FB5A36FEE55694AF116A57CB8.1_cid341?__blob=publicationFile&v=6

(13) https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Emotet-Warnung_230919.html

(14) https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html

(15) https://www.stern.de/digital/online/emotet--darum-ist-der-trojaner-so-gefaehrlich---und-so-schuetzen-sie-sich-8548334.html

(16) https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/BSI_warnt_vor_Emotet.html

(17) https://www.heise.de/security/meldung/Trojaner-Alarm-BSI-warnt-vor-zunehmenden-Emotet-Angriffen-4537594.html

(18) https://siliconangle.com/2019/08/05/ibm-report-finds-destructive-malware-attacks-doubled-since-january/

(19) https://www.sentinelone.com/blog/robinhood-ransomware-coolmaker-function-not-cool/

(20) https://securityintelligence.com/posts/from-state-sponsored-attackers-to-common-cybercriminals-destructive-attacks-on-the-rise/

(21) https://www.welivesecurity.com/deutsch/2016/12/13/12-sicherheitstipps-zur-weihnachtszeit/

(22) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

(24) https://www.heise.de/newsticker/meldung/Mehr-Hacker-Angriffe-auf-kritische-Infrastruktur-beim-BSI-gemeldet-4311172.html

(25) Phishing-Statistik aus dem Hornetsecurity Security Lab

Quellen

(26) https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2019.pdf?__blob=publicationFile&v=4

(27) https://monitor.itskritis.de/ITSKRITIS_Monitor_2_digital.pdf

(28) https://www.it-daily.net/it-sicherheit/cyber-defence/20434-cyberangriffe-kuenstliche-intelligenz-als-fluch-oder-segen

(29) https://www.wissenschaftsjahr.de/2019/neues-aus-der-wissenschaft/das-sagt-die-wissenschaft/kuenstliche-intelligenz-schutzschild-und-einfallstor-fuer-cyberattacken/

(30) https://www.eco.de/presse/internet-security-days-2019-mit-ki-cyberangriffe-abwehren/

(31) https://www.eco.de/presse/das-sind-die-it-security-trends-2019/

(32) https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/07/Report_AI_in_Cybersecurity_Capgemini_Research_Institute.pdf

(33) https://www.computerwoche.de/a/datenschutz-in-microsoft-office-365-ist-lueckenhaft,3546637

(34) https://www.recordedfuture.com/top-vulnerabilities-2018/

(35) https://businessinsights.bitdefender.com/microsoft-phishing-attacks-increased-250-from-january-to-december-2018

(36) https://www.beazley.com/news/2018/beazley_breach_insights_april_2018.html

(37) https://www.secureworldexpo.com/industry-news/new-business-email-compromise-statistics-bec