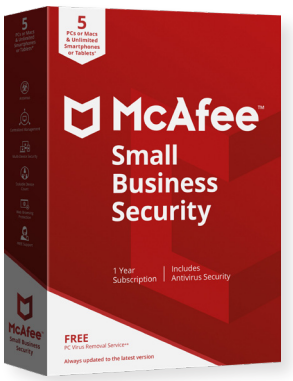
WHITEPAPER

Clevere Sicherheitstipps für kleine Unternehmen

Laut einer aktuellen Studie von Verizon waren 53 Prozent aller kleinen Unternehmen schon einmal Opfer eines Cyberangriffs[1].

Cybersicherheit hat in vielen Unternehmen inzwischen einen hohen Stellenwert, was angesichts der Menge an Datenschutzverletzungen und Ransomware-Angriffen, über die groß in den Medien berichtet wurde, keine Überraschung ist.

Bedrohungen wie etwa der Ransomware-Angriff, der dazu führte, dass städtische Mitarbeiter in den USA monatelang ohne Computer und Smartphones auskommen mussten, oder der Denial-of-Service-Angriff, durch den Rokenbok Education vollständig von der Onlinewelt abgeschnitten war, können durchaus beängstigend sein.



Das gilt insbesondere für kleine Unternehmen, bei denen es häufig keine klare Trennung zwischen geschäftlichen und privaten Informationen gibt. Ein Beispiel wäre etwa ein Unternehmer, der seine private Kreditkarte auch für geschäftliche Zwecke verwendet. Eine Datenpanne ist in diesem Fall doppelt schlimm und wirkt sich unter Umständen nicht nur auf die Finanzen des Unternehmens, sondern auch auf die Finanzen der Familie des Unternehmers aus.

Darüber hinaus nimmt die Anzahl von Angriffen mit potenziell schädlichen Auswirkungen auf Unternehmen zu.

Von McAfee wurden beispielsweise allein im dritten Quartal des letzten Jahres 900.000 neue Phishing-Websites registriert und das Unternehmen merkt an, dass bei neuen Malware-Angriffen[2] sogar das geistige Eigentum unterschiedlichster Unternehmen gefährdet sein kann, wovon unter anderem auch Unternehmen im produzierenden Gewerbe betroffen sind.

Die Berichterstattung in den Medien wird zwar von Großangriffen auf große Unternehmen dominiert, doch gerade kleine Unternehmen sind besonders gefährdet, da sie nur selten über spezielle IT-Mitarbeiter verfügen und häufig bei Phishing-Angriffen ins Visier genommen werden.

Ein Beispiel hierfür ist der Autohändler Green Ford Sales. Angreifer verschafften sich Zugang zum Netzwerk des Händlers und stahlen 23.000 USD von dessen Bankkonto. Doch damit nicht genug: Sie schleusten auch noch neun fingierte Mitarbeiter in die Gehaltsabrechnung ein, was den Händler weitere 63.000 USD kostete.

Noch besorgniserregender als die Häufigkeit der Angriffe auf kleine Unternehmen ist vielleicht eine aktuelle Statistik der National Cyber Security Alliance, in der es heißt, dass 60 Prozent aller kleinen Unternehmen[3], die Opfer eines Hackerangriffs werden, innerhalb von sechs Monaten ihr Geschäft aufgeben müssen. Dies ist in erster Linie kostenbedingt. Laut einer 2019 durchgeführten Continuum-Umfrage entstehen kleinen Unternehmen durch Cyberangriffe im Schnitt Kosten in Höhe von knapp 54.000 USD4 (einschließlich der Kosten für die Bereinigung und die Unterbrechung der Geschäftstätigkeit).

Daher ist es wichtig, dass sich kleine Unternehmen vor derartigen Bedrohungen schützen, bevor es zu spät ist. Achten Sie dazu auf Folgendes:

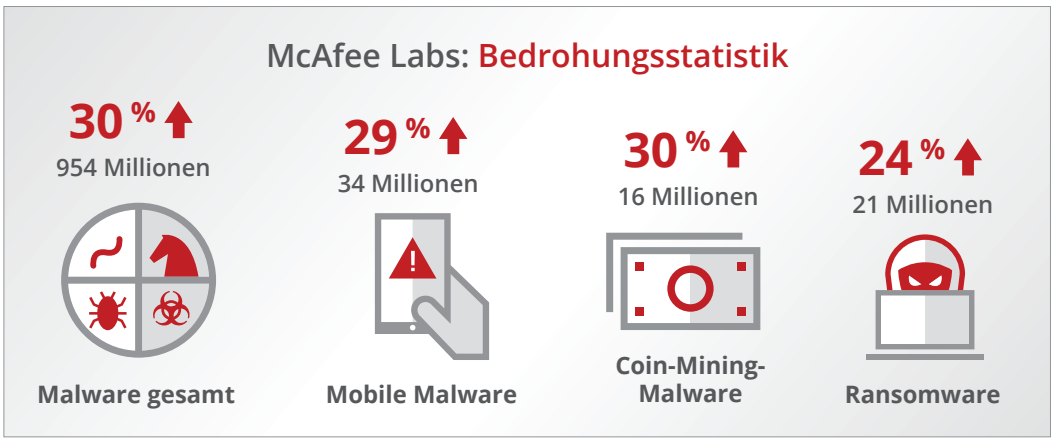
Amtlich aussehender Spam

Unternehmen erhalten immer wieder seriös aussehende E-Mails von Behörden, in denen sie zu einer Zahlung oder zur Angabe vertraulicher Informationen aufgefordert werden. Manche enthalten vielleicht sogar Ihre korrekte Identifizierungsnummer.

Wenn Sie jedoch auf eine solche Nachricht klicken, wird möglicherweise eine gefährliche Website geöffnet, die dazu dient, Ihre Informationen und Ihr Geld zu stehlen, oder womöglich sogar Malware auf Ihren Computer oder auf Ihre Geräte

Die drei wichtigsten Vorteile von McAfee Small Business

- Schutz vor Viren, Ransomware und Malware
- Zentralisierte Lizenzverwaltung
- Bestens geeignet für gemischte BYOD-Umgebungen (Bring Your Own Device)



[5] Quelle: McAfee Labs, 1. Quartal 2019: Bei allen Prozentangaben handelt es sich um Zunahmen der vergangenen vier Quartale.

Allgemeine Bedrohungen für kleine Unternehmen

- Ransomware
- Verlust oder Diebstahl von Geräten
- Gefahren durch BYOD (Bring Your Own Device)
- DDoS-Angriffe (Distributed Denial-of-Service)

heruntergeladen. Gleiches gilt bei fingierten Lieferungen sowie bei betrügerischen E-Mails, deren Empfänger dazu aufgefordert werden, auf Google-Dokumente des Unternehmens zuzugreifen. Diese gezielten Angriffe sind erfolgreich, da sie alltägliche Arbeitsaktivitäten imitieren.

Spear-Phishing (oder „Whaling“)

Eine weitere verbreitete Bedrohung für kleine Unternehmen stellen zielgerichtete Phishing-Angriffe (so genanntes „Spear-Phishing“) dar. Hierbei sendet ein Betrüger eine E-Mail, die scheinbar von einer anderen Person im Unternehmen stammt, und fordert vertrauliche Informationen an – etwa den Verdienst und die Sozialversicherungsnummer von Mitarbeitern, Administratorkennwörter oder Kundendaten. Da diese gefälschten E-Mails von einer Autoritätsperson zu kommen scheinen (beispielsweise vom CEO oder Buchhalter des Unternehmens), geben Mitarbeiter die vertraulichen Informationen häufig weiter, ohne nachzufragen.

Ransomware

Ein einziger unbedachter Klick reicht bereits aus, um Ihr kleines Unternehmen der Gefahr eines Ransomware-Angriffs auszusetzen. Bei Ransomware handelt es sich um schädliche Software, die Ihren Computer sperrt und eine Art Lösegeld fordert, damit Sie wieder auf Ihre Dateien zugreifen können. Das Lösegeld muss häufig in Form von Bitcoins bezahlt werden, da diese nicht nachverfolgt werden können. Es gibt jedoch keine Garantie, dass Ihre Dateien nach der Zahlung tatsächlich wieder entsperrt werden.

Verloren gegangene Laptops/Geräte

Eine verbreitete Sorge unter Inhabern kleiner Unternehmen ist der Verlust oder Diebstahl eines Laptops oder Geräts mit wichtigen Arbeitsinformationen wie etwa dem geistigen Eigentum des Unternehmens. Daher ist es wichtig, über Sicherheitstools zu verfügen, die es ihnen ermöglichen, verloren gegangene Geräte zu lokalisieren und vielleicht sogar per Fernzugriff zu sperren.

Gefahren durch BYOD (Bring Your Own Device)

Da nicht alle kleinen Unternehmen über die finanziellen Mittel verfügen, um Mitarbeiter mit Firmencomputern und -geräten auszustatten, erlauben viele Unternehmen den Mitarbeitern die Verwendung ihrer persönlichen Geräte. Dies wird als „Bring Your Own Device“ bezeichnet. Durch BYOD können kleine Unternehmen zwar zunächst Kosten sparen, ohne entsprechenden Schutz der persönlichen Geräte müssen sie dafür jedoch später unter Umständen teuer bezahlen. Ist also beispielsweise das Gerät eines Mitarbeiters mit Malware infiziert, kann sich diese ganz einfach im Büronetzwerk verbreiten, sobald der Mitarbeiter eine Verbindung herstellt.

DDoS-Angriffe (Distributed Denial-of-Service)

Webbasierte Unternehmen sind der Gefahr eines DDoS-Angriffs (Distributed Denial-of-Service) ausgesetzt. Hierbei überlasten Cyberkriminelle den Server, das Netzwerk oder die Anwendung eines Unternehmens mit Datenverkehr, um einen Ausfall zu provozieren oder sich Zugang zu wertvollen Unternehmensdaten zu verschaffen. Diese Angriffe gibt es schon ziemlich lange. Begünstigt durch die große Menge an Internetbots, die zur Generierung von Datenverkehrsspitzen genutzt werden, war Anfang 2019 jedoch ein Comeback dieses Angriffstyps zu beobachten. Achten Sie daher darauf, dass Ihr Unternehmen stets geschützt ist.

Die Berichterstattung in den Medien wird zwar von Großangriffen auf große Unternehmen dominiert, doch gerade kleine Unternehmen sind besonders gefährdet, da sie nur selten über spezielle IT-Mitarbeiter verfügen.

Wir haben sieben praktische Tipps für Sie zusammengestellt:

1. Schützen Sie Ihr Unternehmensnetzwerk.
   Ändern Sie das Standardkennwort Ihres Routers. Diese Standardkennwörter sind häufig in Hackerkreisen bekannt und können verwendet werden, um sich Zugang zu Ihrem Netzwerk zu verschaffen. Eine entsprechende Anleitung finden Sie im Handbuch Ihres Routers. Stellen Sie sicher, dass die über Ihr Netzwerk übertragenen Daten von Ihrem Router verschlüsselt werden. Und verwenden Sie eine Firewall, um unbefugten Zugriff zu blockieren.

2. Verwenden Sie Kennwortmanager.
   Sorgen Sie dafür, dass alle im Unternehmen einen Kennwortmanager verwenden, um den Verlust und Diebstahl von Kennwörtern zu vermeiden. Mit dieser äußerst nützlichen Software können sichere Kennwörter generiert und sicher gespeichert werden.

3. Löschen Sie sämtliche Software und Anwendungen, die Sie nicht verwenden.
   Dadurch sind Sie weniger anfällig für potenzielle Sicherheitslücken.

4. Sorgen Sie für sicheres Surf- und E-Mail-Verhalten.
   Verwenden Sie ggf. eine Web-Advisor-Lösung auf allen Ihren Computern, um Mitarbeiter bei der Vermeidung riskanter Websites und gefährlicher Downloads zu unterstützen. Darüber hinaus empfiehlt es sich, mit Mitarbeitern über Phishing-Risiken zu sprechen und sie dazu zu animieren, verdächtige E-Mails zu melden, auch wenn es sich um unternehmensinterne E-Mails zu handeln scheint.

5. Halten Sie Ihre Software auf dem neuesten Stand.
   Stellen Sie sicher, dass sämtliche Software auf Ihren Servern und Geräten auf dem neuesten Stand ist, um sie vor bekannten Bedrohungen zu schützen. Dies gilt auch für die Website und die Anwendungen Ihres Unternehmens. Beachten Sie alle Benachrichtigungen, die Sie ggf. im Zusammenhang mit Updates oder Sicherheitsproblemen erhalten.

6. Nutzen Sie umfassende Sicherheitslösungen.
   Investieren Sie in Software (beispielsweise Small Business Security von McAfee) und in Hardware sowie in Latitude-Laptops von Dell mit Sicherheitschip und Fingerabdruck-Lesegerät, um Ihr Netzwerk vor aktuellen Bedrohungen zu schützen. Nutzen Sie ein VPN für die Verschlüsselung privater Browsingservices, um dafür zu sorgen, dass alle Ihre Onlineaktivitäten und -informationen privat bleiben und selbst in einem öffentlichen Wi-Fi-Netzwerk oder in offenen Netzwerken vor Cyberkriminellen geschützt sind.

7. Pflegen Sie eine sicherheitsorientierte Kultur.
   Sprechen Sie mit Ihren Mitarbeitern über verbreitete Sicherheitsrisiken und entwickeln Sie Pläne zur Risikominimierung. Falls bei Ihnen BYOD (Bring Your Own Device) erlaubt ist, stellen Sie sicher, dass alle Geräte, die eine Verbindung mit Ihrem Netzwerk herstellen, geschützt sind. Darüber hinaus sollten Sie Ihre Mitarbeiter über die neuesten Betrugsversuche informieren, damit alle wissen, worauf sie achten müssen.

Partnerschaft zwischen McAfee und Dell

Dank einer Partnerschaft zwischen Dell und McAfee können kleine Unternehmen nun Hardware bestellen, auf der McAfee Small Business Security bereits vorinstalliert ist, und so von Vorteilen wie Spamkontrolle, Tools für die sichere Suche und dem Schutz mehrerer Geräte sowie von der Möglichkeit zum Nachverfolgen oder Sperren eines verloren gegangenen oder gestohlenen Geräts bzw. zum Löschen der darauf befindlichen Daten profitieren – all das und vieles mehr von einem zentralen, benutzerfreundlichen Ort aus.

Informationen zu McAfee

McAfee bietet Device-to-Cloud-Cybersicherheit. Inspiriert von der Kraft der Zusammenarbeit entwickelt McAfee Lösungen für Unternehmen und Privatanwender, um unsere Welt sicherer machen. www.mcafee.com

Informationen zu Dell Technologieberatern für kleine Unternehmen

Dell Technologieberater für kleine Unternehmen arbeiten täglich mit Millionen von kleinen Firmen, Unternehmern und Innovatoren auf der ganzen Welt zusammen. Als zuverlässige Partner für kleine Unternehmen können sie Sie bei der Wahl der passenden Sicherheitslösungen für Ihre Technologie unterstützen. Setzen Sie sich am besten gleich unter 0800-000 94 83* mit einem Dell Technologieberater für kleine Unternehmen in Verbindung.

[1] Verizon-Untersuchungsbericht zu Datenschutzverletzungen (2019).

[2] IDC Vertical Insights-Umfrage (2018).

[3] Vistage: Cyberbedrohungen und Lösungen für kleine und mittelgroße Unternehmen.

[4] Vanson Bourne wurde von Continuum mit den Untersuchungen für den Bericht zum Stand der Dinge bei der Cybersicherheit für kleine und mittelgroße Unternehmen im Jahr 2019 beauftragt. Die Untersuchungen wurden zwischen Januar und März 2019 durchgeführt.

[5] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

DELL Technologies

McAfee™
Together is power.

0800-000 94 83*
*Mo-Fr 8:30-17:30 Uhr
(bundesweit zum Nulltarif aus dem dt. Fest- und Mobilfunknetz)
www.mcafee.com
https://www.dell.com/de