Nicht nur was für Nerds!

Miriam Veith

Redakteurin

Im Schnitt verbringen Menschen in Deutschland 24 Jahre, 8 Monate und 14 Tage ihres Lebens im Internet. Verglichen mit der durchschnittlichen Lebenserwartung, die hierzulande bei etwa 81 Jahren liegt, macht die Internetnutzung also für jeden von uns fast ein Drittel der gesamten Lebenszeit aus. Entsprechend sind Apps und sonstige Online-Dienste aus unserem Alltag definitiv nicht mehr wegzudenken. Trotzdem werden hiermit verbundene Sicherheitsrisiken nur allzu gern ignoriert oder zumindest nicht genügend ernst genommen. Diese laxe Einstellung öffnet Hackern natürlich viele (virtuelle) Türen und Tore. Denn Cyberkriminelle verfügen über eine Vielfalt ausgefeilter Techniken und sind sehr erfinderisch bei der Entwicklung neuer Methoden. Entsprechend schnell werden Zugangsdaten oder persönliche Daten ausspioniert, Dateien und Daten verschlüsselt, um Lösegeld zu erpressen oder sogar die Kontrolle über das ganz System übernommen. Angesichts dieser Sorglosigkeit ist die Bedrohungslage durch beispielsweise Computerviren auf einem gefährlich hohen Niveau angekommen. Mehr als jeder zweite Onliner (55 Prozent) war im vergangenen Jahr Opfer von kriminellen Vorfällen im Internet – ein Anstieg von 5 Prozentpunkten im Vergleich zum Vorjahr.

Aber nicht nur einzelne Privatpersonen geraten immer wieder in das Visier von Hackern. Auch Unternehmen stellen für Cyberangriffe äußert attraktive Ziele dar – erst recht in Zeiten von Homeoffice. Im Jahr 2020 verursachten Cyberattacken bei deutschen Firmen einen historisch hohen Schaden in Höhe von 52 Milliarden Euro. Ein Viertel dieser Schadenszunahme lässt sich gemäß einer Studie des Instituts der deutschen Wirtschaft (IW) auf die Arbeit im Homeoffice zurückführen.

Beliebtestes Ziel der Cyberkriminellen? Banken, Sparkassen und andere Finanzdienstleister. Denn schließlich verfügen diese über eine große Menge sowohl an Kapital (hoffentlich) als auch sensibler Daten, die als das Öl des 21. Jahrhunderts gelten. Laut dem aktuellen Global DNS Threat Report für das Jahr 2021 von Efficient IP und International Data Corporation sind neun von zehn Finanzinstituten weltweit DNS-Attacken wie Phishing, DDoS-Angriffen oder DNS-basierter Malware zum Opfer gefallen. Und das nicht nur einmal: Im Laufe des Jahres 2020 sah sich jedes Finanzunternehmen mit durchschnittlich 8,3 Cyberattacken konfrontiert. Zur Abwehr eines Angriffs wurden im Schnitt 6,12 Stunden benötigt, spürbar mehr als bei Unternehmen aus anderen Branchen. Der besondere Reiz der Finanzdienstleistungsindustrie für die Cyberkriminellen zeigt sich auch in den entstandenen Schäden. Diese sind gegenüber 2019 zwar von 1,16 Millionen Euro auf 884 000 Euro pro Angriff gesunken, liegen damit aber immer noch ein gutes Stück über den durchschnittlichen Kosten in allen anderen Branchen, die sich auf 779 000 Euro je Schadensfall belaufen. Eine erschreckende Bilanz!

Angesichts der zunehmenden Zahl von Fällen, die mitunter prominent in den Medien breitgetreten werden, ist es durchaus überraschend, dass die Kunden ihre Daten bei ihrer Bank oder Sparkasse immer noch in Sicherheit wähnen. Einer Umfrage des Gesellschaft für Konsumforschung GfK zufolge sind sechs von zehn Deutschen (61 Prozent) überzeugt, dass Kundendaten bei Banken und Sparkassen gut oder sehr gut vor unerlaubten Zugriffen geschützt sind. An einen ähnlich verlässlichen Schutz bei großen Internetunternehmen wie Google, Amazon oder Facebook glaubt hingegen nur jeder zehnte Befragte. Skeptisch sind Kunden auch bei Fintechs, denen nur 17 Prozent mit Blick auf sorgfältigen Schutz der Daten vertrauen. Doch drohen natürlich mit jedem weiteren Angriff von außen größere Reputationsschäden, das von den Banken und Sparkassen mühsam und über lange Zeit aufgebaute Kundenvertrauen steht auf dem Spiel.

Höchste Zeit also, sich noch stärker als bislang um das Thema IT-Sicherheit zu kümmern. Da

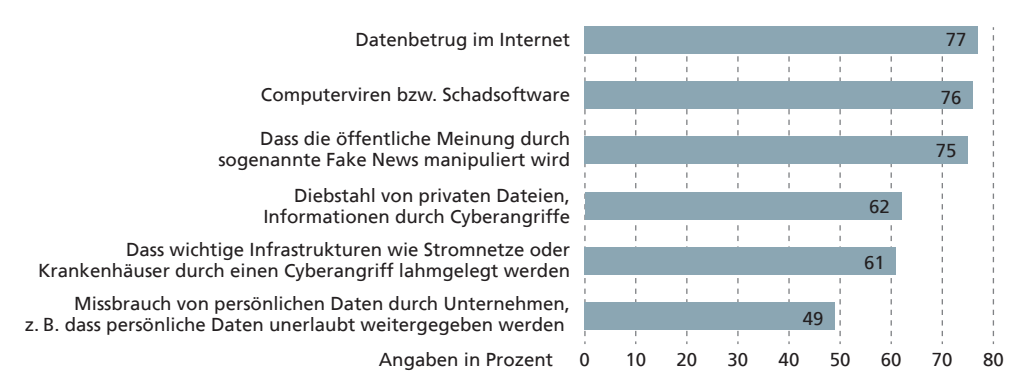
Finanzinstitute ein favorisiertes Angriffsziel der Kriminellen sind, müssen gerade jene an vielen Stellschrauben weiter nachjustieren. Das sieht offensichtlich auch die BaFin so und hat Mitte August die aktuelle Novelle der Bankaufsichtlichen Anforderungen an die IT, kurz BAIT, veröffentlicht. So wird in der Erweiterung nun klargestellt, dass das übergeordnete Ziel bei der Bekämpfung von Cyberkriminalität nicht nur bloß IT-Sicherheit heißen kann, da sich dieser Begriff lediglich auf das Handlungsfeld der Informationstechnik beschränkt, sondern vielmehr in Richtung Informationssicherheit erweitert werden sollte, die den Schutz aller relevanter Informationen zum Ziel hat und somit ein deutlich größeres Handlungsfeld einschließt. Für das Informationssicherheits- und Informationsrisikomanagement heißt das laut BaFin, dass „die betroffenen Unternehmensprozesse ihre Wirkung für die gesamte Organisation entfalten müssen und es nicht ausreicht, allein den IT-Betrieb und die Anwendungsentwicklung mit angemessenen Ressourcen auszustatten".

Des Weiteren haben BaFin und Bundesbank höhere Anforderungen für Wirksamkeitskontrollen wie Schwachstellenscans oder Penetrationstests ebenso formuliert wie an die Protokollierung von Ereignissen und die Überwachung in Echtzeit. Und es wird in den neuen BAIT ausdrücklich gefordert, dass sich die Institute nicht nur über aktuelle externe und interne Schwachstellen informieren, sondern auch die Geschäftsleitung über die Ergebnisse ihrer Risikoanalyse unterrichten.

All diese Anforderungen klingen durchaus vernünftig, setzen allerdings ein gewisses Know-how nicht nur der IT-Spezialisten voraus. Aber auch hier hat die BAIT eine klare Forderung parat: Die Institute sollen ein umfassendes Programm zur Schulung und Sensibilisierung aller Beschäftigten mit Blick auf das Thema Informationssicherheit entwickeln. Die Umsetzung eines derartigen Programms wäre geradezu begrüßenswert. Viele Bankangestellte fühlen sich beim Thema Cyber Security nämlich überhaupt nicht verantwortlich und wollen auch nichts über IT-Technik oder die möglichen Folgen wissen. Sie überlassen dieses Feld gerne alleinig ihren IT-Experten. Doch gerade hier liegt der Casus knacksus: Denn nicht selten haben Cyberangriffe eine menschliche Komponente. Das heißt, dass auch der beste technologische Schutz wenig nützt, wenn Mitarbeiter (meist unabsichtlich wegen Unkenntnis) durch Fehlverhalten das eigene System sabotieren. Deswegen sollte ein Mindestmaß an inhaltlichem Verständnis von IT-Sicherheit zu den Skills eines jeden Bankers gehören. Das ist nicht nur was für Nerds!

Und es dürfte den ein oder anderen sogar in Erstaunen versetzen, dass die Grundlagen von Cybersicherheit kein Hexenwerk darstellen und auch für Laien in relativ kurzer Zeit erlernt werden können. Und viele Kunden möchten ihre Bank beim Thema Sicherheit gerne an ihrer Seite wissen: So hätte laut einer Untersuchung des digitalen B2B2C-Marktplatz Etvas unter 5000 Bundesbürgern jeder Vierte Interesse an einem Anti-Virenschutz-Programm, das der Finanzdienstleister ihnen als Extraservice anbietet. Jeder Fünfte würde auch einen Service nutzen, der alle Geräte auf Sicherheitslücken überprüft und Datenlecks ausfindig macht. Sich als Finanzinstitut umfassend mit Cyber Security zu beschäftigen, kann sich also aus verschiedenen Perspektiven betrachtet nur lohnen!

Bedrohungen durch Cyberkriminalität



Ergebnisse des aktuellen Cyber Security Report 2021, für den Deloitte und das Institut für Demoskopie Allensbach mehr als 400 Führungskräfte aus Unternehmen sowie über 100 Abgeordnete aus den Landtagen, dem Bundestag und dem Europaparlament zum Stand der Cybersicherheit in Deutschland befragt haben.

Quelle: Deloitte