bankenverband

Blog

Cyberkriminalität: Gefahr aus dem Netz steigt – Tipps zum Schutz

01.10.2021

von

Beller, Tanja

Schlagworte

Cybersicherheit
Verbraucher
Cyberattacken
Unternehmen
Cyberkriminalität
Phishing
Kontoauszug
ECSM
Kreditkarte
Onlinebanking
Verbraucherschutz
Sicherheit Verbraucher

bankenverband

Blog

Blog

Weltweit nimmt die Bedrohung durch Cybercrime zu. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht in seinem aktuellen Bericht zur IT-Sicherheitslage von einer „angespannten Situation“. Staaten, Institutionen, Unternehmen und auch jeder private Internetnutzer kann täglich Zielscheibe eines Cyberangriffs werden. Jeder sollte sich der Gefahr bewusst sein und durch sein eigenes Verhalten zu seinem digitalen Schutz beitragen.

Millionen neue Schadprogramme

Insbesondere Cyberangriffe durch Schadprogramme nehmen weiter zu. Allein im vergangenen Jahr wurden laut BSI mehr als 117 Millionen neue Schadprogramm-Varianten registriert – im Durchschnitt mehr als 300.000 pro Tag. Wie gelingt es den Angreifern trotz aller technischen Abwehrmaßnahmen, trotz Aufklärung und Sensibilisierung, schadhafte Programme auf PC, Tablet oder Smartphone zu installieren? In den meisten Fällen durch die Unachtsamkeit von uns Internetnutzern selbst – als Privatperson, als Verbraucher, als Angestellte von Unternehmen oder Institutionen. Zu oft klicken wir vorschnell auf Links, öffnen unbekannte Anhänge, lassen uns schlimmstenfalls zur Eingabe persönlicher, sensibler Daten verleiten, oder laden gar unbewusst eine Software aus dem Netz von unbekannter Quelle herunter – obwohl wir es eigentlich besser wissen sollten.

Installiert werden die schädlichen Programme dann meist unbemerkt. Damit sie vom System nicht erkannt wird, schalten sie teilweise die persönliche Firewall oder das Antivirenprogramm ab. Wenn das gelingt, können Angreifende die Kontrolle über alle Funktionen und Dateien der infizierten Geräte erlangen. Nicht selten wird dies mit einer digitalen Erpressung verbunden.

Fälle digitaler Erpressung nehmen deutlich zu

Als Ransomware werden solche Schadprogramme bezeichnet, die Daten und Systeme verschlüsseln, damit nicht mehr darauf zugegriffen werden kann. Die Angreifer fordern anschließend ein Lösegeld (Englisch: „ransom“) – häufig in Form einer Kryptowährung. Erst nach Zahlung wird der Computer wieder freigegeben. Krankenhäuser, Universitäten, die öffentliche Verwaltung und große Unternehmen wurden bereits Opfer solcher Ransomware-Angriffe. Es kann aber auch kleine Betriebe treffen, denn inzwischen wird Ransomware durch Phishing-Angriffe auch in der Breite gestreut.

Phishing und Spear-Phishing bleibt große Bedrohung

Mit massenhaft versendeten Phishing-Mails versuchen Cyberbetrüger aber auch direkt persönliche Informationen und Zugangsdaten, zum Beispiel zum Online Banking „abzufischen“. Um an eine TAN zu gelangen, die für einen Überwei-

sungsauftrag mit der Zwei-Faktor-Authentifizierung nötig ist, rufen sie ihre Opfer z.B. als vermeintliche Bankangestellte oder Technik-Supportmitarbeiter an. Immer wieder wird auch versucht, über eine Fernwartungssoftware Zugang zum Computer zu erhalten. Ziel der Kriminellen ist es dabei, die Bankkunden dazu zu bringen, eine Zahlung per TAN freizugeben. Selbst wenn nur ein Bruchteil der Empfänger darauf reinfällt, lohnt sich das Geschäft schon für die professionell organisierten Angreifer.

Eine spezielle Variante ist das sogenannte „Spear- (Engl. für Speer) Phishing“. Dabei gehen die Kriminellen gezielt gegen einzelne Opfer vor: Mit Informationen, die vorher ausgespäht oder im Netz gesammelt wurden, versuchen sie Angestellte von Unternehmen zu Überweisungen auf fremde Konten zu verleiten. Den ahnungslosen Angestellten wird dabei oft vorgegaukelt, es handle sich um einen eiligen und besonders vertraulichen Auftrag vom Chef oder der Chefin.

Offene Unternehmenskultur kann zum Schutz vor Hackerangriffen beitragen

Als Mitarbeiter oder Mitarbeiterin eines Unternehmens sollte man sich deshalb nie scheuen, nachzufragen: Bei der IT-Abteilung, wenn man sich unsicher über den Inhalt einer Mail ist, oder bei den Vorgesetzten, um sich eine Zahlungsanweisung nochmal bestätigen zu lassen. Wichtig ist auch eine offene Unternehmens- und Fehlerkultur, die Angestellte darin bestärkt. Denn ist ein Rechner erstmal von einer Schadsoftware befallen, hilft es zumeist nur, ihn komplett neu zu installieren. Ist gar das gesamte Unternehmensnetz infiziert, muss es möglicherweise stillgelegt werden. Zu den unmittelbaren finanziellen Schäden des Betriebsausfalls können erhebliche Reputationsschäden hinzukommen.

Zehn Basistipps zum Schutz vor Hackerangriffen:

1. Führen Sie alle Sicherheitsupdates der Betriebssysteme, Anwendungsprogramme und Antivirensoftware umgehend durch.
2. Speichern Sie auch als privater Nutzer wichtige Daten regelmäßig auf externen Datenträgern.
3. Prüfen Sie den Absender kritisch, bevor Sie auf einen Link klicken oder einen Dateianhang öffnen. Lassen Sie sich nicht vorschnell vom Inhalt dazu verleiten oder unter Druck setzen.
4. Haben Sie den Eindruck, dass Ihr Gerät von einem Schadprogramm befallen ist, schalten Sie es sofort aus. Bestätigt sich der Verdacht, hilft meist nur eine Neuinstallation. Ziehen Sie einen IT-Experten hinzu. Sind Sie tatsächlich Opfer eines Angriffs, melden Sie den Fall bei der Polizei bzw. erstatten Sie Anzeige.

5. Verwenden Sie unterschiedliche und komplexe Passwörter.
6. Speichern Sie keine persönlichen Daten wie PINs oder Passwörter – auch nicht verschlüsselt – auf PC, Tablet oder Smartphone.
7. In öffentlichen W-Lan-Netzen könnten Ihre Daten ggf. mitgelesen werden. Seien Sie sich dessen bewusst und entscheiden Sie umsichtig, welche Daten Sie dort eingeben.
8. Prüfen Sie vor der Eingabe Ihrer Online-Banking-Zugangsdaten, ob die Webdresse im Browser korrekt ist und ob es sich um eine geschützte und verschlüsselte Seite handelt (erkennbar u.a. am Schlosssymbol und der Zeichenfolge „https://“ im Browser).
9. Gehen Sie vorsichtig mit Ihren persönlichen Daten um. Es gilt das Prinzip der Datensparsamkeit. Hinterlassen Sie im Internet nur so viele Informationen wie nötig.
10. Checken Sie regelmäßig Ihre Kreditkartenabrechnungen und Kontoauszüge. Bei Unstimmigkeiten wenden Sie sich direkt an Ihre Bank.

Aufklärung und Sensibilisierung als Daueraufgabe

Wir vom Bankenverband informieren seit Jahren über Cybersicherheit. Der Schutz persönlicher Daten im Netz ist ein wichtiger Bestandteil unserer Verbraucheraufklärung und unser Beitrag zur Betrugsprävention im digitalen Raum. Deshalb unterstützen wir auch in diesem Jahr wieder den European Cyber Security Month (ECSM) – den europäischen Aktionsmonat zur Cybersicherheit.