Freitag, den 6. März 2026

Wie man sich gegen Cyberangriffe schützen kann

Interview. Die Angriffe von Internetkriminellen nehmen zu und werden professioneller. Ihre Erfolgschancen können Privatleute und Unternehmen aber durch einfache Maßnahmen deutlich reduzieren

Von Marco Meng

Alexandre Dulaunoy leitet das Computer Incident Response Center Luxembourg (CIRCL), eine Art „Feuerwehr für Cybersecurity", eine staatlich getriebene Initiative, die Sicherheitsvorfälle sammelt, analysiert, meldet und auf sie reagiert.

Alexandre Dulaunoy, welche Cyberangriffe sind derzeit am häufigsten – und warum?

Phishing hat sich weiterentwickelt, aber es ist immer noch eines der großen Themen, zumindest für Endverbraucher. Unternehmen sind da etwas besser gewappnet.

Auffallend ist, dass es vermehrt Vishing gibt, also Betrugsversuche mit der Stimme. Die Leute werden von jemandem angerufen, der sich als Bank oder Finanzdienstleister ausgibt und versucht, von den Endbenutzern Verifizierungs-Token zu erhalten. Das ist normalerweise gut gemacht, es hört sich tatsächlich wie ein Callcenter der Bank an, aber man sollte da skeptisch sein: Wie wahrscheinlich ist es, dass die Bank einen anruft?

Das ist eine der gängigsten Methoden, die für den Angreifer ziemlich einfach ist. Für Opfer bedeutet das eine Menge finanzieller Probleme, wenn andere Zugang zu ihren Bankkonten haben und dort Überweisungen tätigen. Denn oft folgen Rechtsstreitigkeiten mit den Banken darüber, wer wo verantwortlich ist.

Das größte Problem ist also nicht so sehr technischer Natur, denn Bank-Webseiten sind gut geschützt. Doch beim Zugang selbst muss der Nutzer agieren. Wenn ein Angreifer Sie dazu bringt, Daten preiszugeben, hat er über die Banking-App vollen Zugriff auf Ihr Bankkonto. Das ist ein Klassiker, würde ich sagen. Oft funktioniert also Phishing mittlerweile über Sprache oder per SMS oder manchmal auch in Kombination.

Und bei Unternehmen?

Hier ist eine häufige Masche Malspam: Der Angreifer kontaktiert Unternehmen, um ihnen mitzuteilen, dass eine Zahlung fällig ist. Das angehängte PDF enthält aber ein Programm, das Fernzugriff auf den Computer erlaubt. Viele kleinere oder mittelgroße Unternehmen haben oft keine Schutzmaßnahmen gegen solche Attacken. Die Software der Täter verschlüsselt Firmendaten und Lösegeld wird verlangt.

Viele Sicherheitslücken wären vermeidbar, würden die betreffenden Dienste regelmäßig und ordnungsgemäß aktualisiert.

Was sind die größten Sicherheitslücken?

Der Großteil der Cyberangriffe in Luxemburg geht darauf zurück, dass Systeme nicht rechtzeitig gepatcht wurden – viele Sicherheitslücken wären vermeidbar, würden die betreffenden Dienste regelmäßig und ordnungsgemäß aktualisiert. In mehreren Fällen mussten wir Organisationen darauf hinweisen, dass sie ein Sicherheitsupdate nicht ausgeführt hatten. Oft ist der Grund, dass viele Organisationen ihre IT-Sicherheitsinfrastruktur an einen ICT-Anbieter auslagern, und der seine Arbeit nicht ordnungsgemäß macht.

So kam es auch in den meisten Ransomware-Fällen, die wir in Luxemburg hatten, am Ende zu einem Rechtsstreit zwischen dem Unternehmen und seinem ICT-Anbieter. Wenn sich ein Unternehmen in einer Situation befindet, in der es seine Daten nicht wiederherstellen kann, ist das ein großes Problem, das sogar den Konkurs des Unternehmens zur Folge haben kann.

Was raten Sie Betroffenen?

Kommt einem etwas merkwürdig vor, oder denkt man sogar, man habe etwas falsch gemacht, etwa auf einen Link in einer E-Mail geklickt oder auf ein Pop-up-Fenster, ist es am besten, wenn man sofort die IT-Abteilung davon benachrichtigt.

Wenn man schnell handelt, kann man einem Angriff entgegenwirken und gegenüber den Angreifern Zeit gewinnen. Und wenn Sie einen IT-Dienstleister haben, der sich um Ihre Sicherheit kümmert, stellen Sie sicher, dass Sie eine Möglichkeit haben, zu kontrollieren, was er getan oder nicht getan hat.

Welche Entwicklungen sehen Sie voraus – werden Angriffe KI-gesteuert, automatisiert und personalisiert sein?

Ich bin kein Zukunftsforscher, aber in den letzten 15 Jahren waren die meisten Angriffe im Grunde gleich. Der einzige Unterschied – und hier könnte die KI den Unterschied machen – ist die Industrialisierung der Angriffe, indem etwa Phishing-Angriffe vollständig automatisiert ablaufen.

Der Computer-Sicherheitsforscher Alexandre Dulaunoy: KI erlaubt es Kriminellen, ihre Angriffe zu industrialisieren.
Foto: Chris Karaba

Auch Tippfehler in einem Phishing-Angriff werden weniger, und Bilder oder Videos können von den Tätern leichter eingesetzt werden. In großen Organisationen, wo man Kollegen zum Beispiel nie persönlich begegnet ist, wird es darum wichtiger, zu verifizieren, dass man tatsächlich mit der Person kommuniziert, mit der man zu kommunizieren glaubt. Auch stellen wir fest, dass viele Menschen heute sogenanntes Vibe Coding betreiben, also Software mithilfe von KI erstellen: Sie entwickeln im Schnellverfahren eine Webanwendung – häufig ohne Sicherheitsgrundlagen zu beachten. Das Ergebnis sind schlecht konfigurierte oder fehlerhafte Anwendungen, die für Cyberkriminelle leicht angreifbar sind.

Welche drei Maßnahmen haben die größte Wirkung für private Internetnutzer, die keine technischen Vorkenntnisse haben?

Ich denke, dass einer der schwächsten Punkte der Benutzer selbst ist, wenn er Anwendungen und Ähnliches installiert. Auch wenn einige der App Stores gut kontrolliert sind – je mehr Software man hat, desto größer ist die Wahrscheinlichkeit, dass man angegriffen wird.

Wenn Sie wirklich Spiele und so etwas haben wollen, würde ich zum Beispiel empfehlen, ein anderes Telefon zu benutzen und sich auf eine Software zu beschränken. Aber wir haben heute Dutzende Geräte wie Smart-TVs, Router und Media-Player, die mit dem Internet verbunden sind. Mein Tipp: Überprüfen Sie, ob Sie wirklich alle diese Zugänge benötigen. Und halten Sie die Software der Geräte stets auf dem aktuellen Stand, was viele Leute nicht tun.

Es wird wichtiger, zu verifizieren, dass man tatsächlich mit der Person kommuniziert, mit der man zu kommunizieren glaubt.

Was ist der häufigste Grund, warum Unternehmen Opfer von Cyberangriffen werden?

Wir sehen da kein eindeutiges Muster. Wir betreiben zusammen mit anderen ransomlook.io, eine Plattform zur Beobachtung von Ransomware-Gruppen. Das Open-Source-Projekt überwacht, was Ransomware-Gruppen tun, und gibt Auskunft darüber, welche Art von Unternehmen kompromittiert wurde: Da ist alles dabei, vom Industrieunternehmen bis zum Zahnarzt.

Welche Mindestmaßnahmen sollte jedes Unternehmen ergreifen?

Die Angriffsfläche, nicht nur von Mobiltelefonen, sondern auch von anderen mit dem Internet verbundenen Geräten zu verringern. Wenn Sie also ein kleines oder mittleres Unternehmen sind und Dritte auf Ihre Netzwerke zugreifen können, dann sollten Sie überprüfen, was sie dort tatsächlich tun und ob diese Fernzugriffe tatsächlich nötig sind.

Ein weiterer wichtiger Aspekt ist, dass man miteinander redet: „Ist das normal? Ist das ein klassisches Verhalten?" Wenn man etwas Verdächtiges sieht, sollte man das auf jeden Fall anderen, zum Beispiel Kollegen, mitteilen.

Die Maschen der Datendiebe

Cyberkriminelle nutzen nicht nur E-Mails, um an Daten zu kommen.

Smishing. Eine SMS von einem vermeintlichen Paketdienst: Die Lieferung ist angeblich nicht zustellbar. Dann ein Link zur Sendungsverfolgung oder zum Bezahlen von Zollgebühren. Auf keinen Fall anklicken. Wer wirklich ein Paket erwartet, sollte die Webseite des Paketdienstes aufrufen. Ähnlich, wenn es um Bankangelegenheiten geht.

Quishing. Falsche QR-Codes in E-Mails, auf E-Ladesäulen oder Parkautomaten leiten auf gefälschte Webseiten. Will man dort seine Gebühren bezahlen, liefert man den Kriminellen seine Bankdaten aus.

Vishing. Bei diesem Phishing per Stimme (engl.: Voice) geben sich Betrüger als Mitarbeiter der Bank oder eines Online-Shops aus. Wird man aufgefordert, Zugangsdaten zu nennen, unbedingt das Gespräch beenden. Geben Sie am Telefon niemals vertrauliche Daten heraus.