Hacker zielen auf die Schwachstelle Mensch

Sicherheit Die Hackerattacke auf das Seuzacher Alterszentrum im Geeren lässt aufhorchen. Doch was können Firmen unternehmen, um sich zu schützen? Eine Einordnung von zwei IT-Experten.

Jonas Gabrieli

Der Trojaner tarnte sich als Bewerbung, um am Montagmorgen ins System des Seuzacher Alterszentrums im Geeren (Azig) einzudringen. «Ein Klassiker», sagt Andreas Wisler, Gründer der Wiesendanger Firma Gosecurity, die sich auf das Testen der Cybersicherheit von Firmen spezialisiert hat.

Oft seien solche Bewerbungen extrem gut gemacht, Passfoto inklusive. Gerne nehmen die Hacker auch Bezug auf aktuell ausgeschriebene Stellen. Auf der Website des Azig sind momentan gleich mehrere Jobs offen.

«Beliebt sind auch angeblich noch offene Rechnungen, die bezahlt werden müssen», sagt Wisler. Die Swisscom oder die Transportfirma DHL würden dabei gerne als Absender missbraucht: «Bekannte Namen, zu denen viele Menschen einen Bezug und Vertrauen haben könnten.» Wenn man dann das PDF öffne, um genauer nachzuschauen, sei es bereits passiert. «Jeder Angriff beginnt heute mit einer sozialen Komponente», sagt Wisler. Der Mensch sei im Alltag oft im Stress oder sonst unter Druck. «Und schon ist geklickt.»

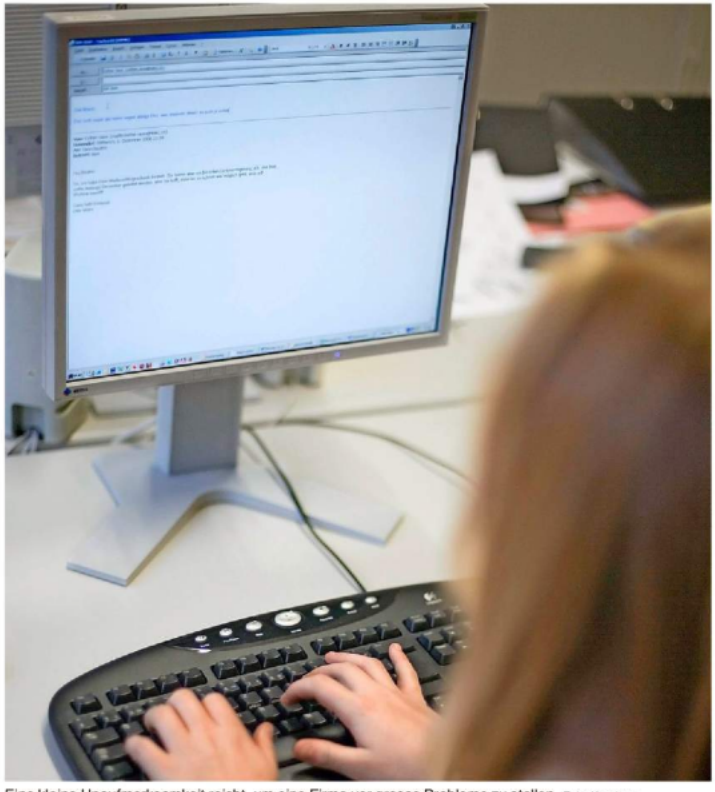
Jeder Zweite tappt in Falle

Denn die Technik ist heute so weit, dass es für die Angreifer extrem schwierig geworden ist, eine Firewall oder einen Server zu hacken. Dass die Angreifer es deshalb oft auf die Schwachstelle Mensch abgesehen haben, bestätigt auch Michael Greuter von der Oberohringer Informatikfirma Vitrodata, die für die IT im Azig zuständig ist: «Oft wird mentaler Druck ausgeübt, indem das Vertrauen ausgenutzt und das Pflichtbewusstsein aktiviert wird.» Besonders perfide: Weil auf gewissen Social-Media-Profilen viele Informationen öffentlich einsehbar sind, können die Hacker diese auf die Zielperson massschneidern. «Da sind richtige Organisationen im Hintergrund, die stetig auf der Suche nach Löchern im System sind.»

Wisler sagt: «Diese Leute nehmen sich Zeit, schiessen nicht einfach drauflos.» Seine Firma schlüpft jeweils in die Rolle der Hacker und erstellt solche massgeschneiderten Phishing-Mails, um Schwachstellen aufzuzeigen. Teils nach einer Schulung zwecks Überprüfung, teilweise aber auch vorher, um auf das Problem aufmerksam zu machen. «Die Klickquote liegt vor einer Schulung jeweils bei 50 Prozent.» Dabei reicht bereits eine Person, die klickt, um eine Firma vor grosse Probleme zu stellen.

Das Azig ist laut Wisler deshalb kein einmaliger Fall. «Die Dunkelziffer ist hoch.» Viele Firmen würden das kaschieren, meist merke man es als Kunde auch nicht, wenn ein System gehackt wurde. Ausser es liegt alles lahm, so wie diesen Sommer bei der Schwerzenbacher Firma Meier Tobler. Dort verschlüsselten Hacker die Systeme so, dass nicht mehr darauf zugegriffen werden konnte. Solche Verschlüsselungen lassen sich normalerweise nicht knacken.

> «Die Dunkelziffer ist hoch.»
>
> **Andreas Wisler**
> Mitgründer der
> IT-Sicherheitsfirma Gosecurity
> Wiesendangen



Eine kleine Unaufmerksamkeit reicht, um eine Firma vor grosse Probleme zu stellen. Foto: Keystone

«Extrem wenig gemacht»

Doch was kann man dagegen tun? Für Wisler ist Datensicherung das A und O. «Es ist die Lebensversicherung der Daten.» Man könnte meinen, das sei mittlerweile selbstverständlich und banal. Doch Wisler widerspricht: «Ich sehe oft das Gegenteil.» Er erzählt von einer Firma, die während Monaten zwar täglich die Back-up-Bänder wechselte, diese wegen eines technischen Fehlers aber stets leer gewesen waren. Beim Faktor Mensch steht hingegen die Sensibilisierung im Vordergrund. Greuter: «Ich muss mich fragen: Mache ich das bewusst? Ist die Forderung realistisch?» Wisler plädiert fürs genaue Hinschauen, bei der Absenderadresse, aber auch bei der Sprache: «Ist das Wort Gruss mit Doppel- oder mit scharfem S geschrieben?» Bei Anhängen soll man generell vorsichtig sein und diese lieber zuerst abspeichern und durch einen Virenscanner laufen lassen, bevor man sie öffnet.

Gesunder Menschenverstand ist beim sogenannten CEO-Fraud gefragt: Dabei wird ein Mail im Namen des Geschäftsführers verschickt, der von der Buchhaltung verlangt, noch rasch einen Betrag auf ein Konto zu überweisen.

Diesbezüglich sieht Wisler noch Verbesserungspotenzial: «Technisch sind die Unternehmen recht weit, aber bei den Schulungen der Mitarbeiter nicht. Es wird extrem wenig gemacht.» Oft hätten die Firmen den Eindruck, dass an ihren Daten niemand Interesse habe. «Das stimmt oft, aber am Geld der Firma schon», sagt Wisler. Oft erscheint nach einer Attacke eine Lösegeldforderung für die Daten auf dem Bildschirm.

Notfallnummer eingerichtet

Der Kampf gegen die Hacker ist laut Greuter ein permanenter Prozess. Eine hundertprozentige Sicherheit sei deshalb eine gewagte Aussage. Er vergleicht es mit dem Einbruchschutz zu Hause: «Es geht darum, Zeit zu gewinnen, den Angreifer möglichst lange aufzuhalten.»

Die Wiesendanger Gosecurity hat angesichts der langsam vorankommenden Cyberstrategie des Bundes vor drei Wochen eine neue Firma namens Swiss Business Protection AG mitgegründet. Über eine Notfallnummer können sich Firmen dort fast rund um die Uhr melden. Die Firma bietet dann die entsprechenden Spezialisten auf. Die beste Massnahme im ersten Moment nach einer erfolgten Attacke? Das Netzwerk trennen, so wie es auch im Azig getan wurde.