DAS INTERNET IST DER WILDE WESTEN

CYBERSECURITY. Wie schützt man sich in Zeiten von Homeoffice und Co vor Hackerattacken? Avi Kravitz, einer der führenden Security-Experten in Österreich, gibt Antworten.

TEXT: Jürgen Philipp

Ein Verteidiger muss schauen, dass alle Fenster und Türen verriegelt sind. Der Angreifer braucht hingegen nur eine einzige Schwachstelle, um einzudringen. Dieses Gleichnis bringt Avi Kravitz, einer der führenden Cybercrime-Experten in Österreich. Gerade das Homeoffice hat Tür und Tor für Cyberkriminalität geöffnet. „Es hat das Thema nach Hause verlagert. Sicherheitskonzepte von vielen Unternehmen greifen nur im Büro. Rund 50 Prozent aller Unternehmen hatten vor Corona keine Homeoffice-Policy." Kravitz skizziert derzeit die beiden größten Cybersecurity-Probleme: „Erstens: Phishing und zweitens Ransomware." Ist Ransomware am Rechner, heißt es meistens: „Bitte bezahlen." Doch wer steckt eigentlich hinter diesen Attacken? „Heute sind rund 70 Prozent aller Hacks finanziell motiviert. Noch vor 15 Jahren war Hacken ein Handwerk, die finanziellen Motive standen noch nicht so im Vordergrund." Mittlerweile gibt es sogar „Cybercrime as a service", in der Cyberkriminelle ihre Dienste anbieten. Kravitz spricht von einer „Underground Economy", in der mit aller Art von Informationen, gestohlenen Daten und Hacking-Tools gehandelt wird. „Es gibt Tools, Anleitungen und sogar einen eigenen Support für Cyberkriminelle."

100 Prozent Schutz gibt es nicht

Unternehmen müssen danach trachten, als Ziel unattraktiv zu werden bzw. zu bleiben. Mittels Software-Updates werden unter anderem auch bekannte Sicherheitslücken geschlossen, auch im Homeoffice. „Im ersten Halbjahr 2020 wurden über 11.000 neue Schwachstellen in verschiedenster Software registriert. Die Softwarehersteller schließen sie mit sogenannten Patches. In der Regel dauert es wenige Stunden bis wenige Tage, bis Hacker sich Zugriff auf nicht ordentlich gepatchte Systeme verschaffen können." Wenn regelmäßig gepatcht wird, reduziert sich so zumindest das Risiko. Denn: „Über 50 Prozent aller Schwachstellen werden für Angriffe genutzt, bevor die Welt sie überhaupt kennt. Das ist allerdings kein Massenmarkt-Problem, sondern betrifft in der Regel nur Menschen und Organisationen, die zielgerichtet von Akteuren ins Visier genommen werden." Ein weiterer wichtiger, oft zitierter Schutz ist die Passwort-Hygiene. „Man sollte für jede Plattform ein eigenes Passwort haben. Dazu kann einem eine Multi-Faktor-Authentifizierung ebenfalls den ‚Arsch retten', wenn man sein Passwort unabsichtlich ‚verloren' hat, und: Setzen Sie immer alle Standard-Passwörter sofort zurück, wenn sie ein neues Gerät aktivieren."

Hirn benutzen

Schließlich rät Kravitz: „Hausverstand benutzen! Das Hirn einzuschalten, ist ein total unterschätzter Faktor. Fast 25 Prozent aller Angriffe starten mit einer Phishing-Mail. Menschen fallen auf eine solche E-Mail herein, öffnen die Anhänge oder geben dort ihr Passwort ein, und schon hat der Hacker Zugang zu ihrem Unternehmens-VPN oder zu Cloud-Diensten." Von den rund 200.000 Domänen, die jeden Tag weltweit registriert werden, dienen rund 70 Prozent kriminellen Zwecken. „Es werden mittlerweile mehr böse als gute Seiten ins Web gestellt." Cybersecurity-Unternehmen wie Blue Shield in Leonding stehen daher sehr hoch im Kurs. Seit Jänner 2020 ist Kravitz bei dem von Alois Kobler gegründeten Unternehmen mit an Bord. „Blue Shield ist ein Meilenstein. Das System ist in 15 Minuten installiert und schützt nachhaltig und verlässlich."

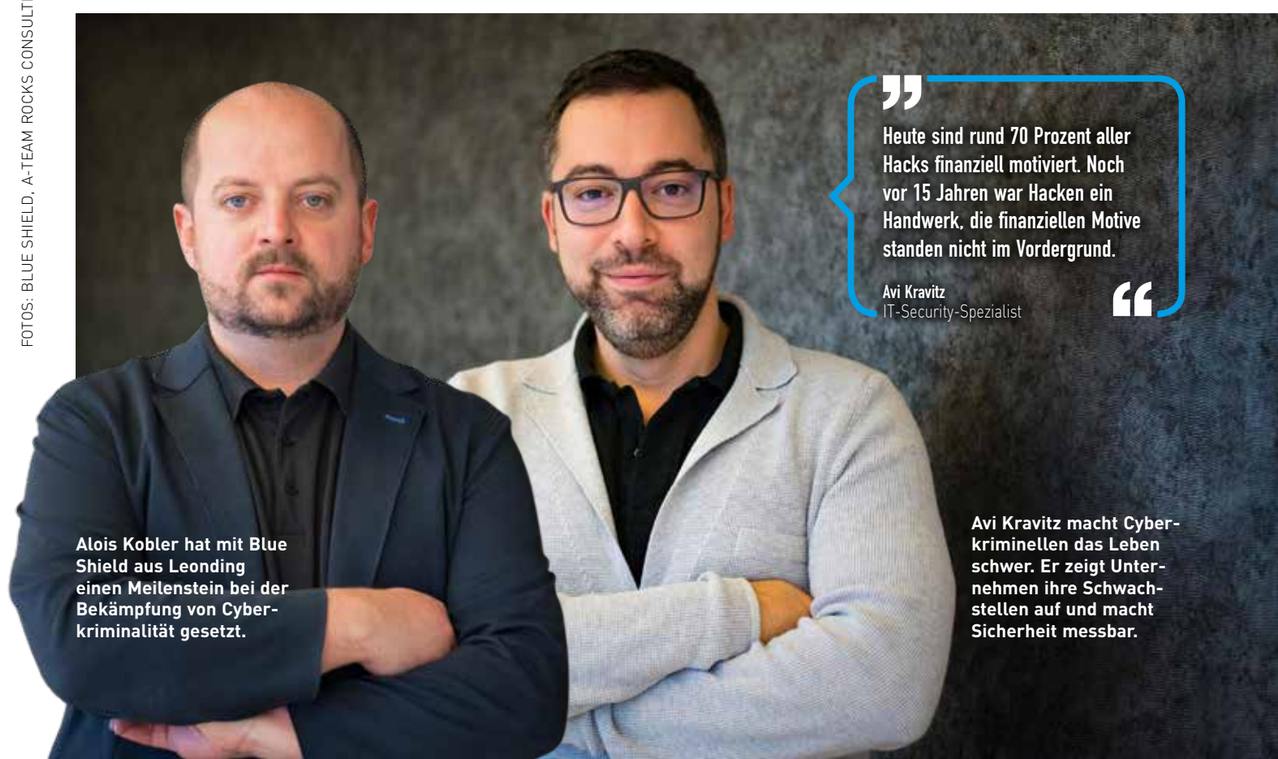
> **Es werden mittlerweile mehr böse als gute Seiten ins Web gestellt.**
>
> **Avi Kravitz**
> IT-Security-Spezialist

Security made in Austria

Blue Shield funktioniert in etwa so: Es gibt eine Deny- oder Blacklist, also eine Liste, auf der steht, was verboten bzw. schädlich ist. „Da es mehr Böses als Gutes im Internet gibt, ist es schwerer, diese Liste aktuell zu halten." Und es gibt eine Allow- oder Whitelist, wo alles zusammengefasst ist, was erlaubt ist. „Blue Shield filtert ausschließlich nach der Allowlist, alles andere wird blockiert. Damit kann niemand mehr auf ein Phishing-Mail reinfallen." Neu registrierte Domänen müssen sich so erst qualifizieren. „Blue Shield schafft einen kritischen Zeitvorsprung von Stunden bis Tagen." Die Software „Made in Austria" mit bereits über 700 Kunden soll zur führenden Lösung in Europa ausgebaut werden. „Wir sind mit unserer Lösung im Herzen Europas technologisch marktführend aufgestellt. Dennoch beziehen öffentliche Verwaltungen eher marketinggetriebene Lösungen aus den USA." Kravitz appelliert daher an die europäische Politik, um europäische IT-Unternehmen und -Startups in Europa zu unterstützen. ■

FOTOS: BLUE SHIELD, A-TEAM ROCKS CONSULTING

FOTO: JUSUN/ISTOCK/GETTY IMAGES PLUS



> **Heute sind rund 70 Prozent aller Hacks finanziell motiviert. Noch vor 15 Jahren war Hacken ein Handwerk, die finanziellen Motive standen nicht im Vordergrund.**
>
> **Avi Kravitz**
> IT-Security-Spezialist

Alois Kobler hat mit Blue Shield aus Leonding einen Meilenstein bei der Bekämpfung von Cyberkriminalität gesetzt.

Avi Kravitz macht Cyberkriminellen das Leben schwer. Er zeigt Unternehmen ihre Schwachstellen auf und macht Sicherheit messbar.