Luzerner Zeitung

abo+ CYBERKRIMINALITÄT

Wie ein Ex-Kommissar gegen Cyberkriminelle kämpft und mit dem Unwillen von Firmen und Institutionen hadert

Chris Eckert prophezeit, dass Cyberangriffe in der Schweiz zukünftig nicht nur Reputation und Geld, sondern auch Menschenleben gefährden könnten. Gerufen wird der Spezialist für Unternehmenssicherheit oft erst, wenn es zu spät ist.

Christopher Gilb

15.09.2021, 11.30 Uhr

Jetzt kommentieren

abo+ **Exklusiv für Abonnenten**

Chris Eckert weiss, bevor der Angriff kommt, sind die Kriminellen oft schon seit 70 Tagen im System.

Bilder: Nadia Schärli (Cham, 13. September 2021)

Es ist nicht einfach, Chris Eckert zu treffen. Der 56-Jährige, der ehemals für die Bundeskriminalpolizei organisierte Kriminalität bekämpfte und nun als Geschäftsführer der Swiss Business Protection AG in Zug Unternehmen in puncto Sicherheit berät, ist derzeit im Dauereinsatz. Grund: die steigende Zahl an Cyberangriffen. Häufig seien die Opfer kleinere und mittlere Unternehmen: «Viele der Firmenchefs denken immer noch: ‹Das

kann doch mir nicht passieren, wir sind doch nur ein kleiner Player, haben gar keine übermässig geheimen Daten, für uns interessiert sich doch keiner›.» Und schon klingle am Freitagnachmittag sein Telefon.

Jeder Angriff sollte interessieren

«Viel zu spät», sagt Eckert. Das sei dann, wenn den Firmen nach einigen Tagen bewusst geworden sei, wie gross der Schaden wirklich ist, dass auch ihr Back-up der Firmendaten beispielsweise ans Netzwerk angehängt ist, das die Erpresser mit ihrer Ransomware blockiert haben. Sie stehen dann mit dem Rücken zur Wand. Und was könne er tun? Oft nicht mehr viel. Versuchen zu verhindern, dass auf die Lösegeldforderung eine zweite folgt, mit Sofortmassnahmen die Reputation des Unternehmens schützen und verhindern, dass so etwas in Zukunft erneut passiert. «Aber eine Firma sicher zu machen, ist keine Sache von einigen Wochen.»

Eckert, Polohemd, Jeans, Kapuzenjacke steht am Ufer der Lorze in Cham. Als das Treffen geklappt hat, schlägt er vor, hier spazieren zu gehen. Wenn er nicht weiter wisse, schaue er oft auf das Wasser. «Ich kann mich dann fokussieren und mir Gedanken machen, mit welchen Strategien sich Unternehmen besser gegen Gefahren schützen könnten.» Die Früherkennung ist das grosse Thema des gebürtigen Aargauers: Das schärft er den Teilnehmenden des von ihm entwickelten CAS Business Protection an der Hochschule für Wirtschaft Zürich HWZ ein. «Wenn ich heute eine kleine Meldung in der Zeitung lese, dass irgendwo ein Stromkraftwerk von Hackern lahmgelegt wurde, dann sollte sich jeder Verantwortliche blitzschnell überlegen: Kann das in meinem Unternehmen auch passieren, haben wir Massnahmen dagegen und wo müssen wir so schnell wie möglich nachbessern?»

Beim Blick aufs Wasser findet Eckert die Ruhe, über Abwehrstrategien gegen drohende Angriffe nachzudenken.

Der Mensch: Die unterschätzte Gefahr

Eckert hat eine Zahl dabei: Gemäss einer aktuellen Studie werden Firmen, bevor der Angriff passiert, im Durchschnitt seit 70 Tagen ausgespäht. «Und viele Firmeninhaber denken noch immer, sie würden schon merken, wenn sie angegriffen werden und könnten rechtzeitig etwas unternehmen. Oder: Unsere IT hat das im Griff.» Das aber sei gerade einer der grössten Trugschlüsse – dass die Verhinderung eines Cyberangriffs eine Frage der richtigen Technik sei. Meistens gehe den Angriffen ein sogenanntes gezieltes Social Engineering voraus. Also dass sich über Beeinflussung und Manipulation von jemandem aus dem Unternehmen Zugang verschafft wird.

«Schauen sie sich mal Geschäftsberichte von Unternehmen an», sagt Eckert. «Jeder will transparent sein und zeigen, was er Gutes tut.» Das sei schön und gut, aber auch gefährlich. «Denn dort oder auch im Internet lassen sich nun Informationen finden, wer welche Funktion im Unternehmen hat, oft noch mit welchem Projekt die Person betraut ist, wer seine wichtigsten Mitarbeiter sind, und natürlich wird auch ein Porträtfoto abgedruckt, manchmal die E-Mail-Adresse.» Und dann erhalte der Mitarbeiter des Finanzchefs ein E-Mail von seinem vermeintlichen Vorgesetzten, er sei ja gerade an diesen wichtigen Verhandlungen und bräuchte schnell die 50'000 Franken, um das Geschäft abzuschliessen. «Das sind Stresssituationen, wer will beim nächsten Qualifikationsgespräch hören, dass er in diesem wichtigen Moment versagt und das Geld nicht schnell genug überwiesen hat.»

Eckert ist ein paar Schritte weitergelaufen. Hündeler laufen vorbei, einmal eine Gruppe Kinder, aber sonst ist nicht viel los an diesem nebligen und eher kühlen Septembermorgen an der Lorze in Cham.

Dass Alarmglocken losgehen, wenn sie losgehen müssen, habe viel mit der internen Kommunikation zu tun, sagt er. Was die Werte im Unternehmen sind, das wüssten die Führungspersonen. «Aber viele weiter unten häufig nicht.» Die Mitarbeitenden müssten deshalb sensibilisiert werden, wovon das Unternehmen lebt. «Also was die Kronjuwelen sind.» Es gehe dabei nicht darum, Misstrauen zu schüren, sondern darum, aufmerksam zu sein: «Mit einem Anrufer nicht leichtfertig über sensible Themen plaudern, in seiner Freizeit genau zu überlegen, wem man was von seinem Job erzählt, wenn jemand ohne Badge im Büro herumläuft, sich zu fragen, wer das ist, und die Person anzusprechen. Man sollte sich bewusst sein, dass der Arbeitgeber potenziell gefährdet ist.» An seinem Haus hänge ja auch niemand eine Anleitung auf, wie eingebrochen werden kann.

Homeoffice als Paradies für Kriminelle

Und vielleicht nicht das Privathandy, mit dem man auch seine Social-Media-Konten betreut, für Firmenkorrespondenzen verwenden? «Das sowieso. Ein Mitgrund, wieso Cyberkriminelle gerade im Hoch sind, ist,

dass während der Coronapandemie Angestellte von einem Tag auf den anderen ins Homeoffice geschickt wurden, etliche noch ohne Firmenlaptops. Es hiess dann: ‹Sie haben ja sicher einen eigenen und können vorerst den nehmen.›» Aus Angst vor Corona, so Eckerts Fazit, sei die Gefahr der Cyberkriminalität teils vergessen worden. Dann sei die geöffnete Bewerbung keine Bewerbung, sondern ein Trojaner gewesen, nur habe das der Privatlaptop der HR-Angestellten nicht erkannt.

Eckert beim gemeinsamen Spaziergang mit Wirtschaftsredaktor Christopher Gilb (links).

Eckert hat noch eine Zahl dabei: «Experten schätzen, dass der Schaden durch Cyberkriminalität bis 2025 auf 10,5 Billionen US-Dollar steigen wird.» Das sei weltweit, aber dass die Schweiz weiter einen starken Anstieg erlebe, bezweifelt er nicht, denn es werde zu wenig unternommen, vor allem von den Unternehmen. «Was wir in unserer Branche seit Jahren nicht verstehen, ist, dass in Unternehmensleitungen, aber auch in Verwaltungsräten, die ja schlussendlich die Gesamtverantwortung tragen, das Thema integrale Sicherheit eine viel zu kleine Rolle spielt.» Vielleicht weil es keine Investitionen seien, die sichtbaren Ertrag generieren, spekuliert Eckert. Dabei sei Sicherheit Chefsache, und der gesamtheitliche Unternehmensschutz müsse Teil der Geschäftsstrategie sein.

Zu wenig unternommen werde aber auch vom Staat. «Was das Thema Wirtschaftsschutz in der Schweiz betrifft, sind wir im Vergleich zu Deutschland mindestens fünf Jahre im Rückstand.» Dort gäbe es wegen der steigenden Zahl an Angriffen beispielsweise ein Kompetenzzentrum Wirtschaftsschutz. Wer sein Unternehmen schützen wolle, erhalte dort wertvolle Tipps und Handlungsempfehlungen. «Gehen sie mal in der Schweiz mit so einem Anliegen zur Polizei, dort gibt es Leute, die sich mit Einbruchsschutz auskennen und ihnen Flyer abgeben, was einbruchsichere Fenster sind, aber Wirtschaftsschutz für Unternehmen gehört leider nicht zu den geforderten Kompetenzen.»

Gesundheitsbranche in Gefahr

Eckerts Bild der Zukunft ist ein düsteres, denn er hat die Vermutung, dass die nächste Branche, die in der Schweiz in den Fokus von Cyberkriminellen rückt, die Gesundheitsbranche ist. Vermehrte Angriffe im Ausland könnten dafür sprechen. «Denn in der Gesundheitsbranche gibt es ein Grundproblem: Ärzte wollen ihre Patienten bestmöglich versorgen, Krankenhäuser wollen aber gleichzeitig möglichst wirtschaftlich sein, also wird nicht an den Geräten gespart, aber vielleicht an anderem.» Und bei so einem Angriff seien dann nicht nur die Firmenkasse oder die Reputation eines Unternehmens, sondern Menschenleben in Gefahr, warnt Eckert. Sein Team und er wollen Gesundheitsinstitutionen frühzeitig unterstützen, bevor es wieder einmal zu spät ist.

0 Kommentare

Alle Kommentare anzeigen

Mehr zum Thema:

Cham Zug Chris Eckert Hochschule für Wirtschaft Zürich Lorze Schweiz Sicherheit Unternehmen

abo+ INTERVIEW

«Lukrativer als der Drogenhandel»: Infoguard-CEO über die rapide Zunahme von Cyberangriffen – und was die Schweiz dringend tun sollte

Interview: Gregory Remez · 29.07.2021