aargau einsA

Der Kanton und seine besten Seiten. 2 2019

ALLES DREHT SICH UM ENERGIE. ENERGIE WIRD GEBRAUCHT, UM ARBEIT ZU VERRICHTEN. ES GIBT VERSCHIEDENE FORMEN DER ENERGIE. ELEKTRISCHE IST EINE VON VIELEN. HYDROTURBINEN NUTZEN DIE ENERGIE VON FLIESSENDEM WASSER UND WANDELN DIESE UM IN STROM. OHNE ENERGIE BEWEGT SICH NICHTS. DER AARGAU LIEFERT ENERGIE, ER IST ENERGIEKANTON.

REIFE IDEEN VERTREIBEN PESTIZIDE

FACHHOCHSCHULE LEHRT UMGANG MIT DATEN

CYBERKRIMINELLE IM NETZ GEFANGEN

Fr. 11.– www.aargau-einsA.ch

DETEKTIVE FAHNDEN IM NETZ

MEHR SICHERHEIT DANK CYBERCRIME-SPEZIALISTEN

Gebäude werden mit ausgeklügelten Alarmsystemen versehen, mit Videoüberwachung und automatischer Alarmierung, Türen mit Chipcodes, Besucher-Badges und elektronischen Zutrittskontrollen – vieles ist im und um das Gebäude bei Unternehmen heute schon selbstverständlich. Anders sieht es bei den IT-Infrastrukturen aus: Sicherheit bleibt hier oft auf der Strecke, und man unterschätzt oft massiv die Gefahr.

Autor: Bruno Wiederkehr

Die Situation lässt sich nicht beschönigen: Angriffe auf IT-Infrastrukturen sind auch in der Schweiz häufig. In den letzten Jahren wurden jährlich rund 5500 Cyberdelikte verübt, wie eine Auswertung der Kriminalitätsstatistik zeigt. Das sind mehr als 100 pro Woche. Dabei geht laut Experten ein grosser Teil auf das Konto professioneller Hacker. Sie legen die Infrastruktur lahm oder schleusen sich ins Computernetzwerk von Firmen ein, spionieren diese aus oder stehlen Daten.

SCHWEIZ EIN TOPZIEL

Die Schweiz ist, wie andere hochindustrialisierte Länder, ein Topziel für Hacker. In Europa liegt – gemäss Handelszeitung – die Schweiz auf Platz drei bei den Cyberattacken, nach Deutschland und Grossbritannien. Weltweit steht die Schweiz auf Rang 7. Und: Die Zahl der Cyberattacken steigt weltweit rasant. Dabei geht es um Technologien, um Produktionsverfahren, aber auch um Kunden-, Preis- und Angebotslisten.

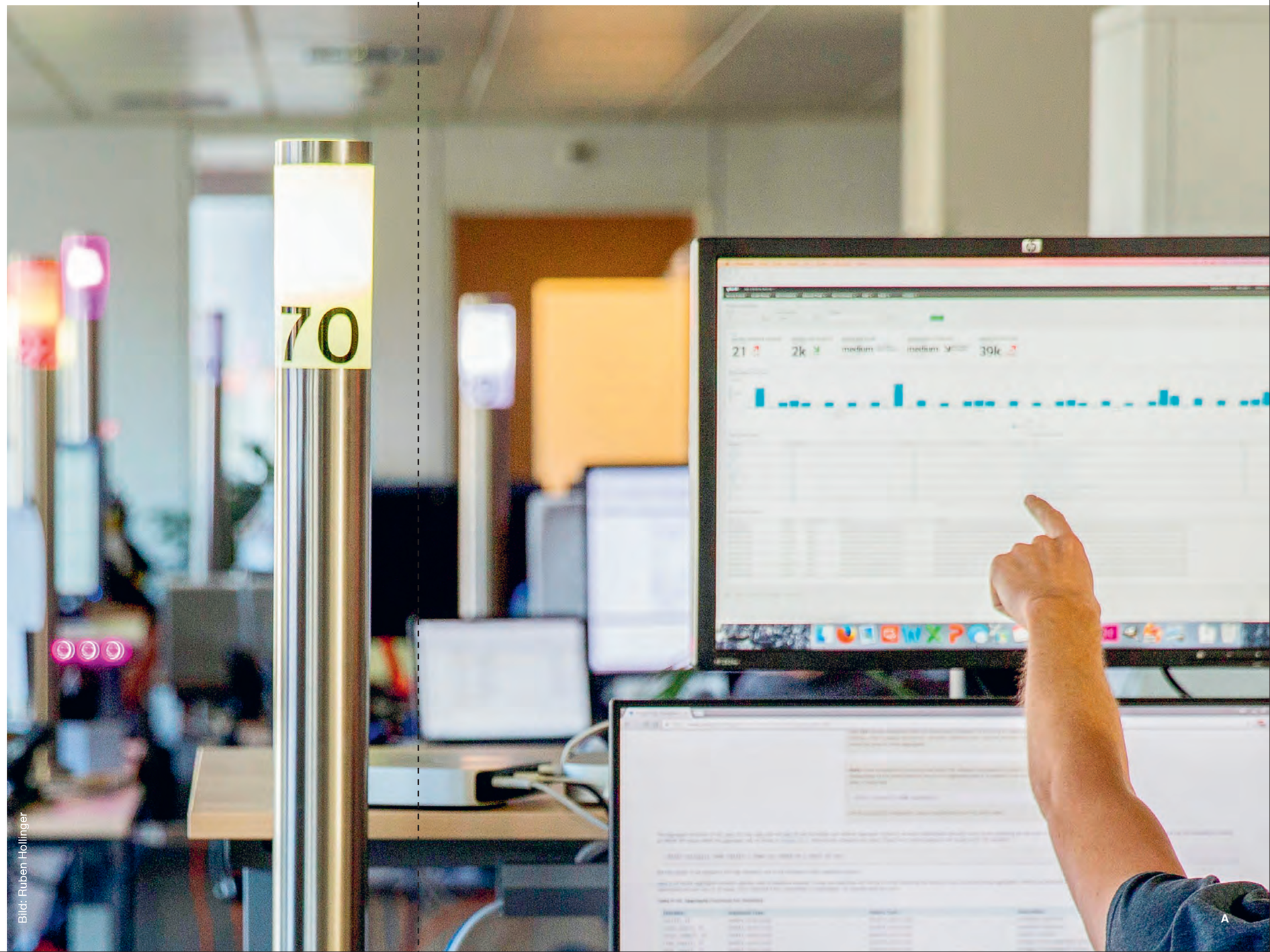

Bild: Ruben Hollinger

B

A Im Security Operations Center der terreActive AG

B Das Managementteam der terreActive AG in der Altstadt von Aarau, in der das Unternehmen seit 1996 seinen Sitz hat.

Die Verluste aus diesen Attacken können teuer bis existenzbedrohend sein. Während die kritischsten Infrastrukturen der Schweiz (u. a. Energie, Transport und Verkehr, Finanzwesen, Rettungsdienste) mittlerweile im Sicherheitsbereich stark aufgerüstet haben, scheinen viele KMU sich der Gefahr noch zu wenig bewusst zu sein.

GESCHÖNTE ZAHLEN

Die offiziell gemeldeten Hackerangriffe sind nur die Spitze des Eisberges. Professionelle Angreifer verwischen ihre Spuren gut und nutzen oft Systeme nichts ahnender Dritter. Oft wird das Datenleck von den betroffenen Firmen auch gar nicht erkannt. Man geht hier von einer riesigen Dunkelziffer aus. Ausserdem wird nur ein Bruchteil der Angriffe überhaupt bemerkt und gemeldet. Hier fürchtet man Reputationsverlust und Auflagen durch Behörden.

FORTSCHREITENDE RISIKEN

Mit der fortschreitenden Digitalisierung in den Unternehmen und den Verwaltungen wird die strategische Aufgabe «Sicherheit» immer komplexer. Ausserdem sind die potenziellen Angreifer den meisten Unternehmen weit voraus: Sie organisieren ihre kriminellen Aktivitäten in spezialisierten Hackerteams. Ihre Angriffe sind schnell und präzise, die Schäden enorm. Schutzmassnahmen alleine genügen längst nicht mehr: Bedrohungslagen müssen untersucht, Angriffe erkannt und Abwehrmassnahmen koordiniert werden. Dazu sind viele Firmen schlicht weder vom Know-how noch von den Systemkenntnissen noch personell und zeitlich überhaupt in der Lage.

SCHWEIZER UNTERNEHMEN OFT ÜBERFORDERT

Während sich auf dem Gebiet der Cyber Security vieles tut, sind Schweizer Unternehmen mit dem Thema strategische IT-Sicherheit zumeist überfordert. Der in Aarau beheimatete IT-Security-Anbieter terreActive hat sein Einsatzteam und das Security Operations Center deshalb stark ausgebaut und in zwei Bereiche gegliedert, um rund um die Uhr mit den Angreifern Schritt zu halten.

DAS SECURITY OPERATIONS CENTER

Das Herz des Unternehmens terreActive ist das Security Operations Center (SOC), das nur durch eine Sicherheitsschleuse betreten werden kann. Hier sorgt man für einen reibungslosen und sicheren Betrieb von über 500 Kundensystemen. Rund um die Uhr, 24 Stunden, 365 Tage im Jahr.

Die Aufgaben des Betriebs wie System Monitoring, Support und Maintenance werden im Operations Control Center (OCC) gebündelt. Hier sind Ingenieure mit dem Betrieb und Unterhalt sämtlicher Sicherheitskomponenten beschäftigt. Insbesondere sind es sogenannte Cyber Security Engineers, welche sich um die Applikationssicherheit kümmern und die Überwachung auf den Kunden und seine Bedürfnisse feintunen.

Ein weiteres Security-Kompetenzteam ist im Incident Response Center (IRC) eigenständig organisiert. Die Spezialisten konzentrieren sich vollumfänglich auf die Überwachung, die aktive Suche nach Schwachstellen und Vorfällen sowie die Koordination der Abwehr. Der Cyber Security Analyst bewertet und analysiert Schwachstellen, erkennt Unregelmässigkeiten, optimiert und verbessert das Alarmsystem.

SPEZIALISTEN GESUCHT

Für all dies braucht es die richtigen Leute. Wie Urs Rufer, CEO der terreActive, betont, sind diese Spezialisten absolute Mangelware und werden händeringend gesucht. «Es ist eine Herausforderung, es mit den raffinierten Hackern aufzunehmen. Es braucht viel Neugier, es braucht Antrieb und eine hohe Motivation. Und bei uns – als Security-Dienstleister für Banken, Verwaltungen, Versicherungen und Institutionen – natürlich auch einen blütenweissen Lebenslauf», unterstreicht er. Oft seien es auch nicht nur die IT-Hochgebildeten ab Fachhochschule und ETH, sondern Quereinsteiger, die sich das notwendige Rüstzeug als Autodidakten zugelegt hätten. Dazu kommen bei terreActive noch die interne Weiterbildung und der wertvolle Austausch innerhalb der Spezialisten.

VERNETZUNG SCHAFFT RISIKO

Die virtuelle Vernetzung von Geräten und Maschinen sowie das wachsende Vertrauen in die Übertragung von Echtzeitdaten auf persönlicher und geschäftlicher Ebene («Internet der Dinge») schaffen weitere Angriffspunkte für Internetkriminalität. Schätzungen zufolge könnten bis 2024 eine Billion Geräte untereinander vernetzt sein; 50 Milliarden Maschinen könnten täglich Daten austauschen. Industrielle Steuerungssysteme stellen ein weiteres Einfallstor für Hacker dar. Ausserdem stammen viele Systemkomponenten aus einer Zeit, als IT-Sicherheit noch keinen hohen Stellenwert hatte. Werden industrielle IT-Systeme durch einen Hackerangriff lahmgelegt, kann dies zu hohen Sachschäden und teuren Betriebsunterbrechungen führen. ★

TERREACTIVE FACTS & FIGURES

_1996 in der Schweiz gegründet
_Über 60 Mitarbeitende
_Davon 45 Ingenieure von namhaften europäischen Universitäten
_Lernende
_Eigene Software-Entwicklungsabteilung

SECURITY OPERATIONS CENTER (SOC)

_Lokal in der Schweiz
_Verfügbarkeit 7 × 24 Stunden
_ISO-27001 zertifiziert für SOC-Services
_Mit Service-Level-Agreement – Reaktionszeit bis zu 15 Minuten