Datum: 02.09.2021

Handelszeitung

Handelszeitung
8021 Zürich
058 269 22 80
https://www.handelszeitung.ch/

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 37'700
Erscheinungsweise: 50x jährlich

Seite: 15
Fläche: 86'887 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 81682502
Ausschnitt Seite: 1/3

Der Cyber-Macher

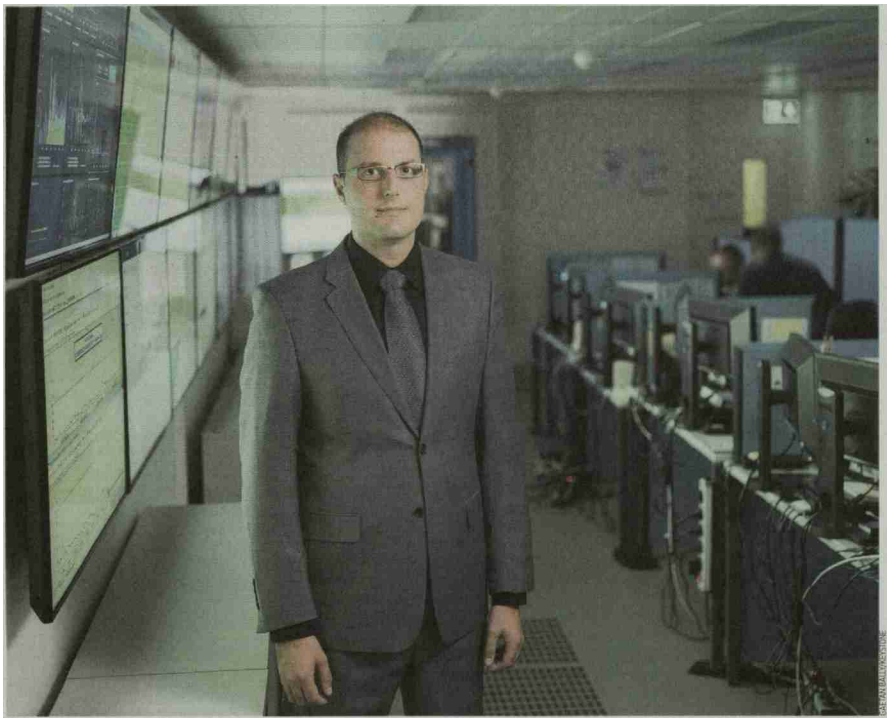
Florian Schütz Er wehrt Angriffe gegen das Land ab und will Automechaniker zu Cyberprofis ausbilden.

BERNHARD FISCHER

Ein Stockwerk mit einer Handvoll Büros, ein paar Computer, Kopierer, Sitzungsräume, 35 Mitarbeitende und 11,2 Millionen Franken Budget. Dies steht dem Chef der nationalen Cybersicherheit, Florian Schütz, zur Verfügung. Von der Berner Schwarztorstrasse aus koordiniert er die Abwehr von Hackern, Kryptoräubern und digitalen Spionen. Wer glaubt, Cybersecurity spielt sich in einem ominösen Kubus mit raumschiffartigem Kommandoraum und bebrillten Computer-Nerds in Uniform ab, irrt.

Schütz ist der Leiter des Nationalen Zentrums für Cybersicherheit (NCSC). Sein Büro ist dem Generalsekretariat des Finanzdepartements angeschlossen. Hier kümmert er sich um die gesamte nationale Cybersicherheit. Schütz versteht seine Arbeit als «präventiv, omnipräsent – und aktiv», darauf legt er Wert. So richtig abschalten will er gar nicht. Zu spannend findet er das Thema IT. Wenn er mal zu einem Buch greift, dann einem über automatisierte Produktion mit Blick auf die Lieferketten. «Man muss ja verstehen, was die Herausforderungen bei vernetzen Maschinen sind.»

In seiner Position als Schweizer Cyberchef arbeitet er mit Exekutivkräften wie auch mit Kontraktoren aus der Privatwirtschaft zusammen. Und vereint ein bisschen von allem in seiner Funktion: Nachrichtendienst und IT, Militär und Polizei, Politik, Wirtschaft und Infrastruktur. Das sind die Bereiche, in denen er und seine Cyberspezialisten vor allem aktiv sind.



Florian Schütz, Leiter des National Cyber Security Centre (NCSC): «Es gibt Defizite.»

Offensive Fähigkeiten

Die Bundesverwaltung, für die Schütz tätig ist, gehört zu den sogenannten kritischen Infrastrukturen. Zu dem Zweck hat er in seiner Funktion bereits mit externen, freundlichen Auftragshackern eine grosse IT-Überprüfung der Parlamentsdienste und des Aussendepartements (EDA) veranlasst – in der Fachsprache wird das Bug-Bounty-Programm genannt. Allein das EDA ist ein Mammutressort mit 6000 Beschäftigten, 170 Aussenstellen in mehr als 100 Ländern und entsprechend exponiert. 15 Hacker und Hackerinnen wurden auf einen bestimmten Teil der Bundes-IT angesetzt, zehn Schwachstellen haben diese gefunden, eine davon ist kritisch. «Wir planen, das in der einen oder anderen Form weiterzuführen», sagt Schütz. Dafür braucht es defensive und offensive Fähigkeiten der Cyberexperten im Auftrag des NCSC. Wo Schüt: die offensive Power noch einsetzen lassen wird, klärt er bereits ab. Wie, wo und wann – darüber darf er nicht sprechen.

Vieles erfährt die Öffentlichkeit gar nicht. «Was mich manchmal irritiert, ist, wenn man in den Medien vernimmt, dass wieder einmal etwas passiert sei, und dann behauptet wird, der Bund habe nicht geholfen.» Checkt Schütz die Cybersysteme des Bundes, dann sieht er, dass die Behörden sehr wohl geholfen haben. Darunter leidet die Sichtbarkeit seines Erfolgs.

Gelernt hat der nationale Cyberchef sein Handwerk an der Uni. Neben dem Studium assistierte er in den Nullerjahren an der ETH in einem Labor, in welchem er das

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch

Datum: 02.09.2021

Handelszeitung

Handelszeitung
8021 Zürich
058 269 22 80
https://www.handelszeitung.ch/

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 37'700
Erscheinungsweise: 50x jährlich

Seite: 15
Fläche: 86'887 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 81682502
Ausschnitt Seite: 2/3

Labornetz sicherte und Studierenden beim Experimentieren mit Angriff und Verteidigung von Computernetzwerken half. Zusammen mit seinen Kolleginnen und Kollegen brachte er die Systeme zum Anschlag und zeigte auf, wie man diese ausnützen kann. Heute nennt man diese Methode Red- und Blue-Teaming, wie man das auch beim NCSC kennt: Ein Team attackiert, das andere verteidigt, aber transparent und unter Aufsicht. «Ich war das Red Team und das Blue Team in Personalunion.»

11,2
Millionen Franken für die Cyberabwehr.

Dann kamen seine ersten Einsätze beim Rüstungskonzern Ruag und aufgrund seiner speziellen IT-Fähigkeiten als Fachoffizier auch bei der Schweizer Armee. Es war jene Zeit, als Cyberthemen so richtig virulent wurden und sogar die Ruag selbst mit Cyberattacken konfrontiert wurde. Ein Cyberangriff 2016 war immerhin ausschlaggebend dafür, dass die Ruag in zwei Unternehmensteile aufgespalten wurde. Wobei: «In den Vorfall 2016 involviert war ich nicht», stellt Schütz klar. Head of Cyber Security bei der Ruag war er in den viereinhalb Jahren davor.

Was Schütz umtreibt, ist die Faszination für Prozesse. Dem fachlichen Umfeld blieb er immer treu, wechselte aber schon mal die Branche. Fast drei Jahre lang leitete er die IT-Sicherheit von Europas grösstem Online-Modehändler Zalando. Das privatwirtschaftliche Umfeld des E-Commerce kennt er daher sehr gut. «Ich weiss, was es bedeutet, wenn man einen Cyber-Incident hat, pro Minute einen fünfstelligen Betrag verliert und mit begrenzten Ressourcen den Schaden minimieren muss.» Bei Zalando habe er Risikomanagement gelernt und wie man Sicherheit skaliert und automatisiert. Nach In- und Auslandeinsätzen für die Ruag als Manager und dem Intermezzo in der Welt des Online-Modehandels kehrte Schütz zur nationalen Sicherheit zurück. Als oberster nationaler Cyberchef ist er auch für die IT der Ruag unverzichtbar geworden. «Ruag International ist eine privatrechtliche Firma, die heute noch als kritische Infrastruktur gilt und Zugang zu den Dienstleistungen des NCSC hat.»

Perfekt läuft es natürlich nie. Zwar stehe die Schweiz in Sachen Cyberschutz derzeit nicht schlecht da, «aber es gibt Defizite». Schütz verliert den Plauderton, wird ernst: «Statt nur Spezialistinnen und Spezialisten auszubilden, bräuchte es Zusatzausbildungen in einzelnen Berufen.» Ein Automechaniker zum Beispiel sollte die Cyberaspekte eines Bordcomputers im Fahrzeug dazulernen. Der Cyberchef würde gerne «eine Workforce herstellen, die mit solchen Kompetenzen international gefragt wäre, damit auch ins Ausland gehen und mit neu erlerntem Wissen und Auslanderfahrung wieder in die Schweiz zurückkommen kann, um Familienunternehmen und KMU fortzuführen oder zu gründen». Noch immer würden zu viele Unternehmen nicht einmal einen gewissen Grundschutz im Griff haben.

Auch im Infrastrukturbereich, bei Stromlieferanten oder der Bahn, müsse die Sicherheit weiter ausgebaut werden. Dafür müssten die Geschäftsleitungen mehr involviert werden. «Bei jenen Infrastrukturen, die wenig Wettbewerb ausgesetzt sind, ist der Schutz meist geringer ausgeprägt», sagt Schütz. «Banken etwa, die viel Geld und ihren guten Ruf verlieren würden, wenn etwas passiert, haben ein deutlich stärkeres Bewusstsein dafür, bis hin zum Verwaltungsrat.»

So rasch wie möglich melden

Und wenn sich eine Attacke mal nicht verhindern lässt, dann müsste das so rasch wie möglich gemeldet werden, findet Schütz. Aktuell ziele eine Meldepflicht für die Privatwirtschaft in der Schweiz nur auf kritische Infrastrukturen ab. «Ich empfehle Unternehmen, dass diese in ihre Lieferantenverträge hineinschreiben, dass sie von ihren Lieferanten informiert werden müssen, wenn ein Cyberangriff passiert.» Eine Online-Meldestelle, bei der man niederschwellig (und freiwillig) melden kann, wurde für Unternehmen bereits eingerichtet.

Mehr Kompetenz, mehr Verantwortung, mehr Meldungen – Schütz referiert die drei Punkte im Stakkato, verleiht den Worten Gewicht. Man merkt: Was die Schweiz in Cyberfragen kann, was ihr fehlt und wie man das Land vor Angriffen sicherer machen kann, ist ihm auch ein persönliches Anliegen.

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG
ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch

Datum: 02.09.2021

Handelszeitung

Handelszeitung
8021 Zürich
058 269 22 80
https://www.handelszeitung.ch/

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 37'700
Erscheinungsweise: 50x jährlich

Seite: 15
Fläche: 86'887 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 81682502
Ausschnitt Seite: 3/3

CYBERCRIME

Zielscheibe für Internetkriminelle

Bandenkriminalität Über 80 Prozent der Cybervorfälle in der Schweiz sind organisierte Kriminalität. Etwa im Bildungsbereich, wo starke Computerinfrastrukturen missbraucht werden für Angriffe ausserhalb der Schweiz – um zum Beispiel unerlaubt Bitcoins zu minen oder für Spionage in Sachen Innovation an Hochschulen.

Datenklau Die Schweiz ist in Europa überdurchschnittlich betroffen von Virus- und Malware-Angriffen. Schon vor Homeoffice- und Pandemiezeiten waren bereits 22 Prozent sämtlicher Internetnutzer und -nutzerinnen von derlei Angriffen betroffen. Der EU-Schnitt liegt bei 16 Prozent. Bei Identitätsdiebstählen liegt die Schweiz europaweit auf Platz zwei hinter Österreich. Während Cyberattacken weltweit überwiegend per E-Mail und Phishing erfolgen, geschieht dies in der Schweiz zu mehr als drei Vierteln direkt über das Netz. Davon sind mehr als zwei Drittel Datenklau. Die meisten identifizierten Angriffe gegen Unternehmen kommen übrigens nicht aus Russland oder China, sondern aus den USA und von innerhalb der Schweiz.

ARGUS DATA INSIGHTS® WISSEN ZUM ERFOLG

ARGUS DATA INSIGHTS® Schweiz AG | Rüdigerstrasse 15, Postfach, 8027 Zürich
T +41 44 388 82 00 | E mail@argusdatainsights.ch | www.argusdatainsights.ch