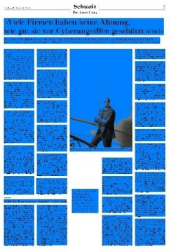
Datum: 20.12.2021

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 87'908
Erscheinungsweise: 6x wöchentlich



Seite: 7
Fläche: 119'993 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 82824824
Ausschnitt Seite: 1/4

«Viele Firmen haben keine Ahnung, wie gut sie vor Cyberangriffen geschützt sind»

Der Bund warnt täglich Firmen, die gerade Opfer einer Hackerattacke werden. Doch die Verantwortung für den Schutz liege bei den Unternehmen, sagt Florian Schütz, Delegierter für Cybersicherheit des Bundes, im Gespräch mit Lukas Mäder und Georg Häsler

Herr Schütz, wie gut sind die Unternehmen in der Schweiz vor Cyberangriffen geschützt?
Ich glaube nicht, dass die Schweiz schlechter dasteht als andere europäische Länder. Aber zwischen den Firmen gibt es grosse Unterschiede bei der Cybersicherheit. Das hängt zum Beispiel davon ab, ob die IT-Sicherheit auf der Stufe Verwaltungsrat und Geschäftsleitung ein Thema ist. Oder von der Branche. Die Banken haben schon früh gemerkt, dass sie zum Beispiel beim Kreditkartengeschäft Geld verlieren, wenn sie zu wenig in ihre Cybersicherheit investieren.

Stehen grössere Unternehmen besser da?
Nicht unbedingt. Aber bei vielen KMU ist das Geld knapp. In der Schweiz gibt es viele Firmen mit einem Umsatz von weniger als einer halben Million Franken. Nimmt man die Budget-Richtwerte, wie viel davon für die IT-Sicherheit eingesetzt werden sollte, kommt man auf 2000 bis 5000 Franken im Jahr. Das ist nicht viel. Der Staat sollte die Rahmenbedingungen so gestalten, dass die Firmen mit dieser kleinen Summe einen grossen Effekt erzielen.

Es gibt die politische Forderung, dass der Bund Gemeinden und Firmen vor Cyberangriffen schützen müsse. Tun Sie heute zu wenig?
Der Bund macht bereits heute viel in diesem Bereich. Das Nationale Zentrum für Cybersicherheit warnt zum Beispiel täglich zahlreiche Unternehmen und Behörden ganz gezielt vor Gefahren. Etwa vor Cyberkriminellen, die auf ihren Rechnern aktiv sind, oder vor Schwachstellen, die wir selbst entdeckt haben oder die uns gemeldet wurden. Die Verantwortung für den Schutz vor Cyberangriffen liegt aber primär bei der jeweiligen Institution.

Wie erfahren Sie davon, dass eine Schweizer Firma von Cyberkriminellen angegriffen wird?
Es kann sein, dass wir Hinweise aus dem In- oder Ausland erhalten oder selbst verdächtige Aktivitäten sehen. Die Ransomware-Gruppen haben Kontrollserver, die teilweise von Polizeien oder Nachrichtendiensten beobachtet werden. Gibt es einen Kontakt zwischen dem Server der Kriminellen und einer Schweizer IP-Adresse, erhalten wir eine Meldung. Wir warnen dann die betroffene Firma oder Behörde und bieten unsere Hilfe an.

So haben Sie zum Beispiel die Uhrenherstellerin Swatch und die Amag-Gruppe über einen laufenden Angriff informiert. Das klingt, als ob es ziemlich einfach wäre, Angriffe frühzeitig zu erkennen.
In den erwähnten Fällen hat die Zusammenarbeit sehr gut funktioniert. Dies ist leider nicht die Regel. Bei Cybervorfällen ist es wichtig, dass man rasch reagiert. Oft erreichen wir aber in der betroffenen Firma niemanden. Dann müssen wir eine Warnung per eingeschriebenem Brief verschicken. Dadurch verlieren wir wertvolle Zeit. Wir empfehlen deshalb allen Unternehmen, auf ihrer Website einen Security-Kontakt anzugeben.

Im Sommer wurde die Gemeinde Rolle Opfer von Cybererpressern. Wie sieht Ihre Hilfe in so einem Fall aus, also wenn der Cyberangriff erfolgreich war?
Ich kann nicht über konkrete Fälle sprechen. Aber der Ablauf ist meist ähnlich. Eine Behörde oder eine Firma merkt, dass sie angegriffen wird und Hilfe braucht. Sie meldet sich bei uns. Für die kritischen Infrastrukturen wie Stromversorger oder Banken sind wir rund um die Uhr erreichbar. Da machen sich unsere Mitarbeitenden auch einmal nachts um 1 Uhr auf den Weg.

Was machen Sie vor Ort?
Wir helfen zu verstehen, was das Problem ist: Welche Schadsoftware wird eingesetzt? Wie können wir verhindern, dass sich die Angreifer ausbreiten? Wir raten den Organisationen jeweils auch, die Polizei einzuschalten und einen externen IT-Dienstleister beizuziehen, wenn sie keine eigene IT-Sicherheitsabteilung haben. Manchmal beraten wir gar bei der Kommunikation.

Und wo hört Ihre Hilfe auf?
Irgendwann ist die Situation unter Kontrolle. Wir ziehen uns zurück und überlassen die Arbeit den internen oder externen IT-Spezialisten. Dann konzentrieren wir uns darauf, die gewonnenen Erkenntnisse für den Schutz anderer Unternehmen zu nutzen. Unsere Unterstützung bei Vorfällen ist vergleichbar mit der Aufgabe einer Feuerwehr: Diese kommt vor Ort, um den Brand zu löschen. Das Aufräumen ist aber nicht ihre Aufgabe.

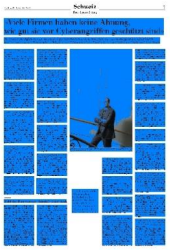
Für wen rückt die Feuerwehr des Bundes aus? Für eine Schreinerei mit zwanzig Mitarbeitern vermutlich nicht.
Wir haben den Auftrag, die kritischen Infrastrukturen zu schützen, wozu auch Gemeinden und Kantone gehören. Aber auch bei einer Schreinerei geben wir

Datum: 20.12.2021

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 87'908
Erscheinungsweise: 6x wöchentlich



Seite: 7
Fläche: 119'993 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 82824824
Ausschnitt Seite: 2/4

Auskunft, raten zum Beispiel, externe Hilfe zu holen und die Polizei einzuschalten. Oder wir verweisen auf die Empfehlungen auf unserer Website.

Sollte der Bund in Zukunft mehr tun können für private Unternehmen, die nicht zu den kritischen Infrastrukturen gehören?

Wir müssen die Erwartung an den Bund in diesem Bereich klären. Es ist sicher möglich, private Unternehmen stärker zu unterstützen. Dafür brauchen wir aber die nötigen Ressourcen und eine rechtliche Grundlage. Ich persönlich bezweifle, dass es nötig und sinnvoll ist, dass der Bund allen angegriffenen Unternehmen direkt hilft. Warum sollte der Steuerzahler für die Sicherheit jeder einzelnen Firma bezahlen? Es gibt private Angebote für solche IT-Dienstleistungen.

«Es gibt immer wieder Schwachstellen, die die Kriminellen ausnützen. Der Bund könnte präventiv nach Systemen in der Schweiz suchen, die diese Lücke aufweisen.»

Ist Sicherheit nicht eine Staatsaufgabe? Bei einem Einbruch kommt auch die Polizei.

Bei einem Cyberangriff sollten die Opfer auch unbedingt die Polizei beiziehen. Wir als NCSC unterstützen die Strafverfolgungsbehörden. Aber der Staat kann nicht die Schadensbewältigung übernehmen.

Was ist denn die Aufgabe des Bundes?

Zurzeit ist der Auftrag an das NCSC stark auf die Unterstützung von kritischen Infrastrukturen ausgerichtet. Ich bin der Meinung, der Bund muss in erster Linie die Rahmenbedingungen schaffen, damit sich die Unternehmen besser selbst schützen können.

Wie zum Beispiel?

Viele Firmen, mit denen ich rede, haben keine Ahnung, wie gut sie bei ihrem Provider vor Cyberangriffen geschützt sind. Wehrt der Provider Attacken von bekannten Angreifern automatisch ab? Wie schnell reagiert er bei einem Vorfall? Muss noch ein zusätzliches Sicherheitspaket gekauft werden? Das sind wichtige Fragen. Aber die IT-Serviceprovider geben nur selten transparent an, welches Sicherheitslevel sie ihren Kunden mitliefern. Deshalb möchte ich im Rahmen der nächsten nationalen Strategie für Cybersicherheit anschauen, ob wir die Serviceprovider zu einem höheren Sicherheitsniveau bewegen können, ohne in den Wettbewerb einzugreifen. Dies könnte zum Beispiel mit einem Label erfolgen.

Es braucht eine bessere Information?

Ich habe die Vision, dass der Bund eine Informationsplattform zur Verfügung stellt für Behörden, Firmen sowie Bürgerinnen und Bürger. Alle Interessierten sollen massgeschneidert jene Informationen erhalten oder abonnieren können, die sie für ihre Aufgabe brauchen. Zusätzlich wollen wir auch besser warnen können.

Gibt es nicht schon genug Warnungen, die dann oft nicht beachtet werden?

Ich denke an eine gezielte Information. Es gibt immer wieder gefährliche Schwachstellen, die die Kriminellen ausnützen. Der Bund könnte präventiv nach Systemen in der Schweiz suchen, die diese Lücke aufweisen.

Der Staat soll überprüfen, ob die Firmen genügend gut geschützt sind?

Es geht nicht um ein komplettes Monitoring. Dies muss auch in Zukunft der freien Marktwirtschaft überlassen werden. Das Monitoring würde nur die Fälle einer erhöhten Gefährdungslage betreffen. So könnten wir die Unternehmen gezielt informieren. Ich halte dies für einen spannenden Ansatz, weil er die Wirtschaft unterstützt, ohne den Firmen ihre Verantwortung abzunehmen.

Haben Sie derzeit genug Stellen im NCSC?

Die Frage ist: genug für welchen Auftrag? Natürlich wird das NCSC noch wachsen müssen. Die Belastung ist zurzeit gross.

Sie haben im Frühling keine zusätzlichen Stellen fürs neue Jahr beantragt, obwohl es eigentlich einen Ausbauplan gab. Warum?

Wir wollen zuerst unsere heutige Organisation analysieren. Das NCSC gibt es seit anderthalb Jahren, und ich bin seit gut zwei Jahren im Amt. Wir wollen schauen, wo wir stehen, was wir erreicht haben und wo wir welche Leistungen erbringen müssen. Mit dem Ergebnis der Analyse werden wir auch Vorschläge machen, wo der Bund weiter ausbauen soll.

Die Armee baut ihre Kapazitäten stark aus mit einem Cyberkommando, in dem auch Milizangehörige dienen. Kann das NCSC bei der Armee Hilfe anfordern?

Ja, ich kann mich bei der Armee melden und Unterstützung anfordern. Wichtiger ist aber, dass ich mich direkt mit den Verantwortlichen über Bedrohungen und mögliche Einsätze frühzeitig austauschen kann.

Wie häufig kommt das vor?

Praktisch nie. Wir hatten im letzten Jahr einmal eine Kooperation im präventiven Bereich. Mit dem Ausbruch der Pandemie gerieten die Spitäler zunehmend ins Visier von Cyberkriminellen. Da haben wir für den Fall eines Angriffs gewisse technische Vorkehrungen getroffen und personelle Reserven gebildet. Die Führung bei diesem Einsatz lag aber klar bei uns.

Es geht bei einer Unterstützung durch die Armee also um grosse Cyberangriffe, die auch über längere Zeit viele Ressourcen binden?

Wir müssen Überlaufgefässe bilden für die Ausnahmesituation. Unabhängig davon, ob wir sie tatsächlich brauchen. Meine Vision ist, dass man die Ressourcen innerhalb des Bundes herumschieben kann, je nachdem, wo sie benötigt werden. Einmal hilft die Armee dem NCSC, einmal umgekehrt. Wir müssen einander unterstützen.

Datum: 20.12.2021

Neue Zürcher Zeitung

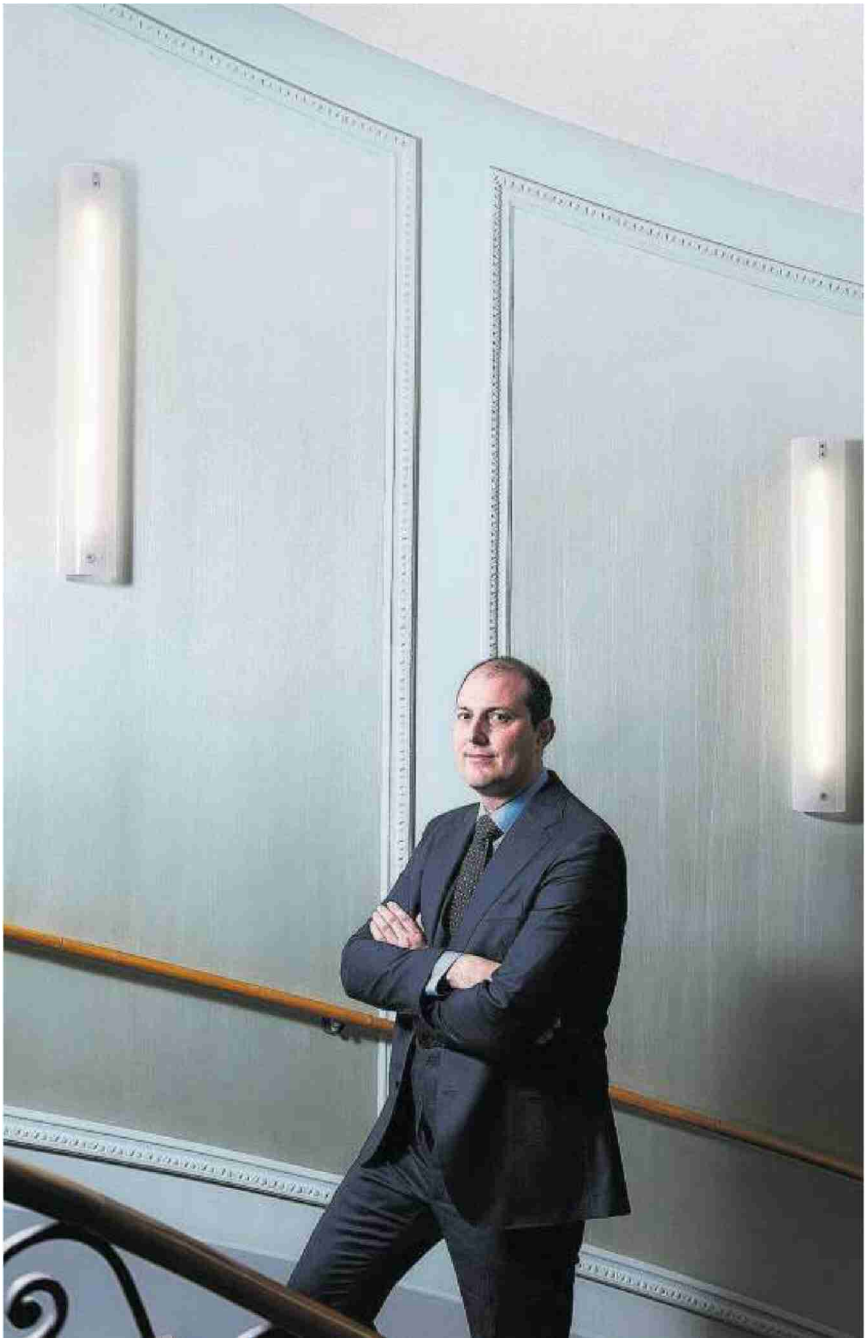
Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 87'908
Erscheinungsweise: 6x wöchentlich

Seite: 7
Fläche: 119'993 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 82824824
Ausschnitt Seite: 3/4



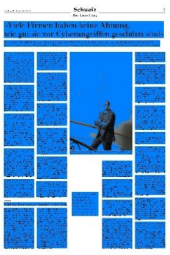
«Die Belastung ist zurzeit gross»: Florian Schütz ist seit August 2019 der Delegierte für Cybersicherheit des Bundes. KARIN HOFER / NZZ

Datum: 20.12.2021

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 87'908
Erscheinungsweise: 6x wöchentlich



Seite: 7
Fläche: 119'993 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 82824824
Ausschnitt Seite: 4/4

Zahl der Ransomware-Angriffe steigt stark

mdr. · Das Problem der Ransomware-Angriffe wird in der Schweiz grösser. Dem Nationalen Zentrum für Cybersicherheit (NCSC) beim Bund wurden in der ersten Hälfte des laufenden Jahres 94 Ransomware-Angriffe gemeldet. Das ist eine Verdreifachung gegenüber dem ersten Halbjahr 2020. Im gesamten letzten Jahr wurden dem Bund 67 Ransomware-Fälle gemeldet.

Ein Grund für die Zunahme dürfte sein, dass die Meldung an den Bund einfacher geworden ist. So hat die Zahl der Meldungen seit der Einführung des neuen Meldeformulars im Januar 2021 in allen Bereichen zugenommen. Ausserdem beobachtet der Delegierte für Cybersicherheit des Bundes, Florian Schütz, dass die Zurückhaltung bei den Firmen, Ransomware-Angriffe zu melden oder öffentlich zu kommunizieren, abgenommen hat. Die Unternehmen sähen, dass sie nicht die Einzigen seien, die es getroffen habe.

Die hohe Zahl an Cyberangriffen in den letzten Monaten hat die Politik aufgeschreckt. Der Bund solle die Cybersicherheit für Gemeinden und KMU sicherstellen, lautet die Forderung. Doch der Bundesrat lehnt dies ab. Um die Verantwortung für den Schutz vor Angriffen zu übernehmen, müsste der Bund bei den Behörden und Firmen Schutzmassnahmen anordnen und überprüfen können, schreibt der Bundesrat in der Antwort auf einen Vorstoss der FDP-Ständerätin Johanna Gapany: «Dies bedeutete einen massiven Eingriff in die Souveränität der Kantone und in die Wirtschaftsfreiheit.»