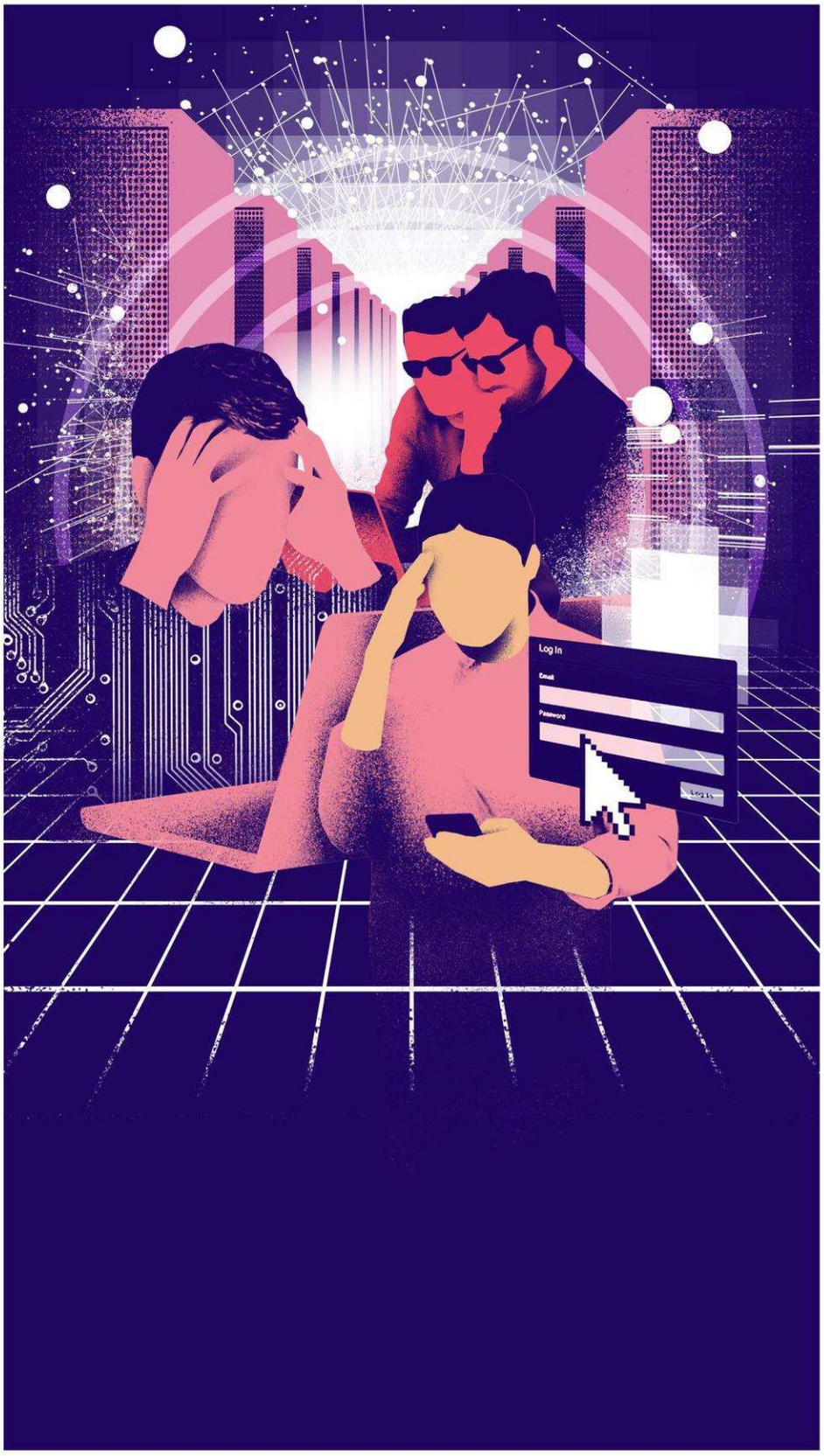
Abo **Cyberkriminelle machen Beute**

So pressen Hacker Millionen aus Schweizer Firmen

Hacking-Attacken mit Verschlüsselungssoftware nehmen zu. In Genf bezahlten gehackte Firmen kürzlich eine Million Lösegeld. Der oberste Cyber-Ermittler warnt vor Bequemlichkeit.



Christian Brönnimann , Sylvain Besson , Svenson Cornehls
Aktualisiert: 05.12.2021, 15:17



Die Zahl der sogenannten Ransomware-Attacken hat sich im Vergleich zum Vorjahr verdreifacht.

Es ist der Albtraum von jedem Unternehmer. Am Montagmorgen in der Früh schalten sich die Server des mittelgrossen Industrieunternehmens in der Zentralschweiz automatisch aus. Die Firmen-Website verschwindet vom Netz. Die E-Mail-Konten der Mitarbeiter sind nicht mehr zugänglich. Auf dem Desktop von einem Computer, der noch läuft, befindet sich nur noch eine Datei: «readme.txt».

Wenn man die Textdatei öffnet, erscheint eine Nachricht, verfasst in schlechtem Englisch. «Welcome», steht da, «your files are encrypted» – Ihre Daten sind verschlüsselt. Es folgt eine Anleitung, wie man vorgehen muss, um sie wieder lesbar zu machen. «It's just a business» – es ist nur ein Geschäft.

Die einzige Datei, die das Zentralschweizer Industrieunternehmen nach dem Hacker-Angriff noch öffnen konnte.

Foto: PD

Die Firma wird auf eine Website der Hacker im Darknet gelotst. Dort ist eine Lösegeldforderung deponiert, zusammen mit einem Versprechen und einer Drohung. Wird das Lösegeld bezahlt, liefern die Hacker die Schlüssel zur

Decodierung der Daten. Wenn nicht, veröffentlichen sie die Daten. Fünf Millionen Dollar sind in diesem Fall gefordert. Viel Geld für das Industrieunternehmen.

Schweiz stärker unter Beschuss als andere Länder

Einen solchen Schockmoment erleben Schweizer Unternehmer immer häufiger. Die Zahl der sogenannten Ransomware-Attacken (Verschlüsselung und Erpressung) ist zuletzt stark gestiegen. 94 Fälle hat das nationale Zentrum für Cybersicherheit im ersten Halbjahr 2021 registriert – dreimal mehr als im Vorjahr. Und das ist nur die Spitze des Eisbergs.

Serdar Günal Rütsche ist Cybercrime-Chef der Zürcher Kantonspolizei und Leiter der nationalen Koordinationsstelle der Polizeikorps für Internetkriminalität (Nedik). Bei ihm laufen die Fäden der Cyber-Ermittlungen in der ganzen Schweiz zusammen. Er schätzt die Dunkelziffer der Ransomware-Attacken auf Schweizer Institutionen auf etwa das Zwanzigfache der registrierten Fälle. Angriffe mit Verschlüsselungssoftware seien zum klar grössten Problem der Internetkriminalität geworden, sagt Günal Rütsche. Die Schweiz stehe gar noch mehr unter Beschuss als andere Länder. «Jede grössere Hackergruppe hat hier schon Opfer gefunden.»

Serdar Günal Rütsche, Cybercrime-Chef der Zürcher Kantonspolizei und Leiter der nationalen Koordinationsstelle der Polizeikorps für Internetkriminalität (Nedik).

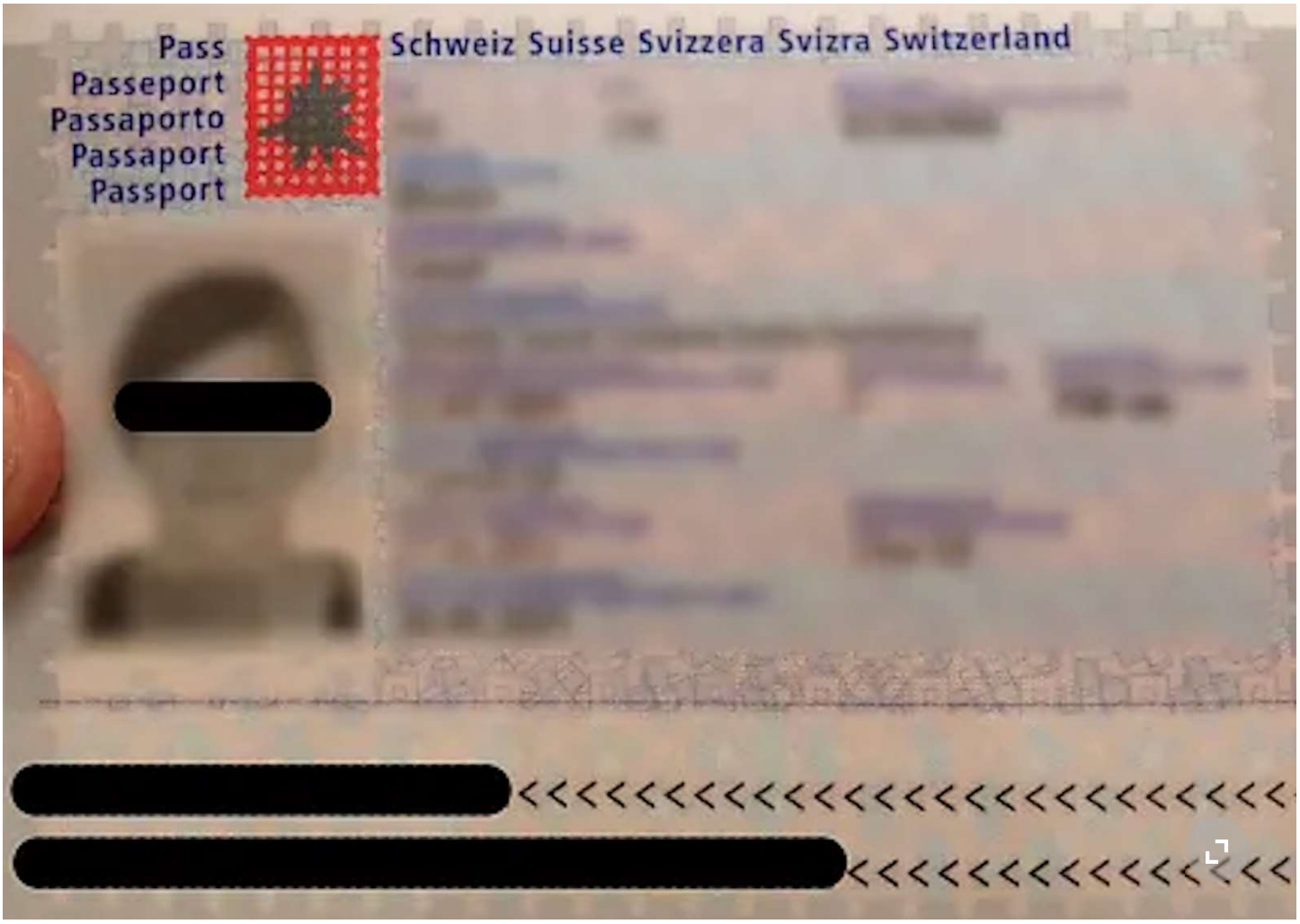
Foto: zvg

Dafür gibt es laut Günal Rütsche zwei Gründe: «Cash und Bequemlichkeit.» Die Hacker wüssten genau, dass Schweizer Unternehmen vergleichsweise liquide seien – und dass es hierzulande oft mehr Sicherheitslücken gebe als anderswo. «Die fehlende Wartung der Systeme ist das eine. Aber wir stellen auch immer wieder fest, dass man nicht auf Komfort verzichten will: Die Verwendung von USB-Sticks, Fernzugriff auf das Firmennetzwerk aus dem Homeoffice oder schlechte Sensibilisierung der Mitarbeiter – all das macht es Kriminellen einfacher, in Computernetzwerke einzudringen», sagt Günal Rütsche.

In der Schweiz fänden die Ransomware-Banden aber nicht nur viele Opfer. Es komme auch immer wieder vor, dass sie ihre Angriffe über Schweizer Infrastruktur ausführten, sagt Günal Rütsche. «Stabile und zuverlässige Infrastruktur und Diskretion sind auch für Kriminelle attraktiv.»

Hochsensible Daten von Alkoholkranken und Arbeitslosen gestohlen

Den Hackern gelingt es bei ihren Aktionen, an immer sensiblere Daten zu gelangen. Nicht nur Firmengeheimnisse sind gefährdet. Kürzlich tauchten im Darknet etwa die Fotos von Pässen von Schweizer Bürgern auf. Sie stammen aus einem Hack gegen das internationale Reisebüro FTI. Von einem Innerschweizer Treuhandbüro gelangten Dutzende Steuererklärungen ins Darknet. Auch Gemeinden, die in ihren Registern die persönlichen Daten ihrer Bürger speichern, waren in den letzten Monaten wiederholt Ziel von Ransomware-Attacken.



Im Darknet tauchten kürzlich Fotos von Schweizer Pässen auf.

Foto: inside-it.ch

Der Bundesrat rechnet mit weiteren solchen Angriffen. «Es muss davon ausgegangen werden, dass auch weitere Gemeinden gegenüber Cyberangriffen verwundbar sind. Der Grund dafür liegt hauptsächlich darin, dass viele Behörden noch über zu wenig Wissen über mögliche Cyberbedrohungen verfügen, um sich effektiv vor solchen Angriffen zu schützen», schrieb er Mitte November in einer Stellungnahme.

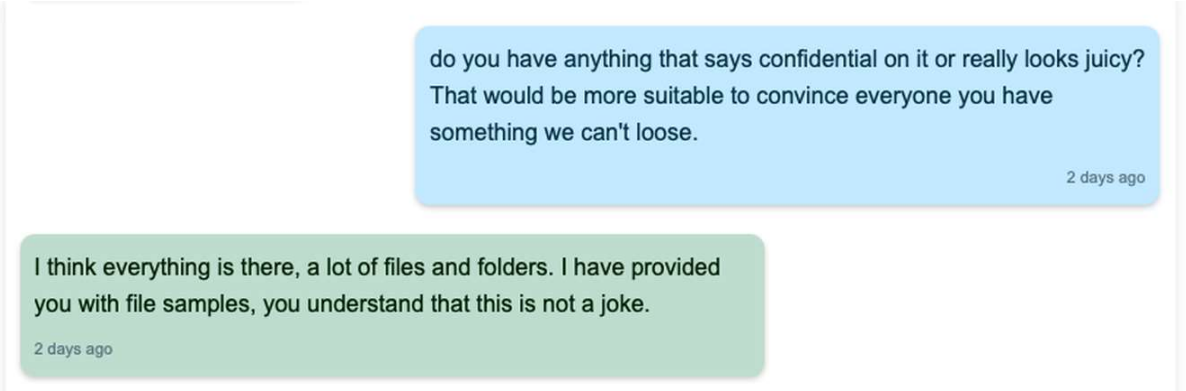
Nun zeigen Recherchen: Im Kanton Waadt gelangten Hacker vor wenigen Wochen an noch heiklere Daten. Nämlich an die einer Stiftung, die Menschen in schwierigen Lebenssituationen bei der Reintegration hilft; Suchtkranke, Arbeitslose oder Hochverschuldete. Man kann es sich vorstellen: Würden die Namen der Klienten öffentlich, hätte das für sie gravierende Konsequenzen.

Die Daten der Stiftung lagen auf dem Server einer externen IT-Firma in Genf, genau wie die ebenfalls gestohlenen Daten von sechs weiteren Genfer Unternehmen, darunter eine Anwaltskanzlei und ein Vermögensverwalter. Sie schätzten das Risiko einer Veröffentlichung des gestohlenen Materials als zu gross ein und bezahlten letzten August knapp eine Million Franken in Bitcoins als Lösegeld an die Hackergruppe Dark Matter.

Ein Drittel bis die Hälfte der Firmen zahlen das Lösegeld

Nicht immer erreichen die Hacker ihr Ziel. Im Fall des Zentralschweizer Industrieunternehmens beispielsweise floss kein Geld. «Das Unternehmen war gut vorbereitet und konnte seine Systeme ohne Schlüssel der Hacker aus Back-ups selber wieder zum Laufen bringen», sagt Mathias Fuchs von Infoguard. Die auf Computersicherheit spezialisierte Firma unterstützt und berät Unternehmen bei Cyberattacken.

Keine drei Stunden nachdem das Industrieunternehmen den Angriff bemerkt hatte, stand Fuchs schon in Kontakt mit den Hackern von der russischen Gruppe REvil. Über eine gesicherte Plattform der Gruppe im Darknet chattete er mit den Cyberkriminellen. Auf seine Frage, ob die Angreifer beweisen könnten, dass sie tatsächlich Daten gestohlen hatten, schickten diese umgehend ein Foto einer Firmenfeier, das sie auf einem der Server gefunden hatten. Danach folgten Geschäftsunterlagen. «This is not a joke», das ist kein Witz, schrieben die Hacker noch, um den Druck zu erhöhen.



Auszug aus dem Chat des Zentralschweizer Industrieunternehmens mit den Cyberkriminellen.
Foto: PD

Doch wirklich sensible Daten hatten sie in diesem Fall nicht erbeutet. Deshalb stufte das Unternehmen den Schaden einer Veröffentlichung als geringer ein als die fünf Millionen gefordertes Lösegeld.

In anderen Fällen versucht Mathias Fuchs, die Lösegeldsumme herunterzuhandeln. «Die Hacker agieren sehr professionell. Sie wissen genau, wie viel ein angegriffenes Unternehmen bezahlen kann.» Normalerweise stiegen sie mit einem Betrag von 3 bis 5 Prozent eines Jahresumsatzes des Unternehmens ein, sagt Fuchs. Oft gelinge es ihm mit einer Mischung aus Gegendruck und Hinhaltetaktik, die Summe um bis zu 70 Prozent zu reduzieren. «Zwischen einem Drittel und der Hälfte der Unternehmen muss am Schluss bezahlen, da die Daten nicht aus Back-ups wiederhergestellt werden können.»

> **«Die Hacker agieren sehr professionell. Sie wissen genau, wie viel ein angegriffenes Unternehmen bezahlen kann.»**
>
> Mathias Fuchs, Infoguard

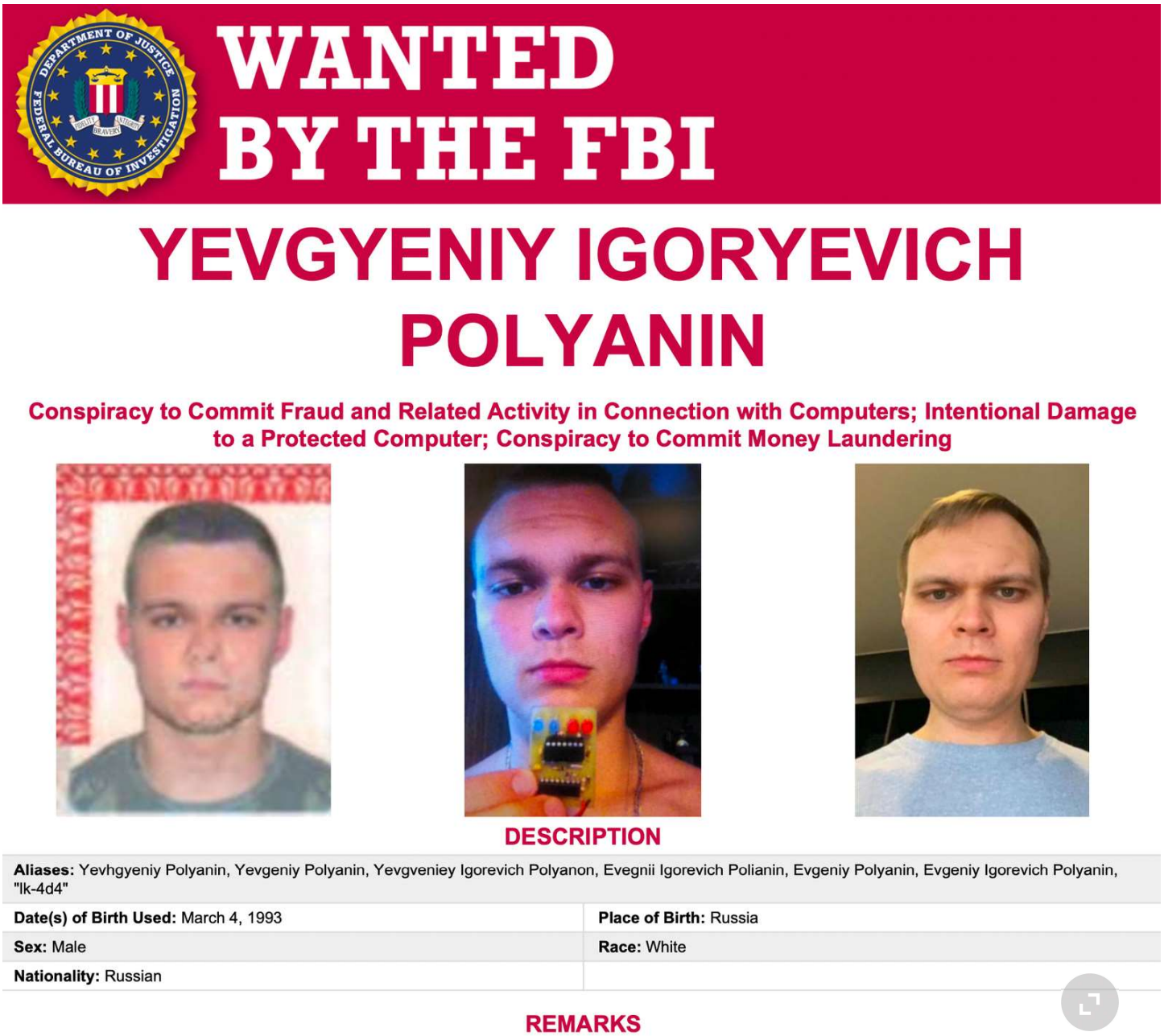
Laut Fuchs treten die Ransomware-Gruppen in den Verhandlungen wie Geschäftsleute auf, die gegen Geld einen Dienst anbieten: den Schlüssel zur Wiederherstellung der Daten und die Zerstörung der gestohlenen Daten. Manchmal lieferten sie als kleines Extra am Schluss sogar einen detaillierten Bericht, wie sie in das gehackte Unternehmen eingedrungen seien, damit dieses davon lernen könne, sagt Fuchs.

Strafverfolger schlagen zurück

Inzwischen haben die Behörden im Kampf gegen die Cyber-Erpresser zugelegt. Weltweit sind Strafverfolgern in den letzten Monaten Schläge gegen grosse Hackergruppen gelungen. In zwei Aktionen waren auch Schweizer Ermittler beteiligt. Dabei verhaftete die Baselbieter Polizei Ende Oktober erstmals eine Person wegen Verdachts auf Beteiligung an einer Ransomware-Gruppe. Die Person ist in Untersuchungshaft, ein Strafverfahren läuft. Die Aktion wurde von Europol koordiniert und richtete sich gegen zwölf teils hochrangige Mitglieder einer Cyberbande, namentlich aus der Ukraine. Sie stehen im Verdacht, fast 1800 Ransomware-Attacken mit Opfern in 71 verschiedenen Ländern durchgeführt zu haben.

Zürcher Ermittler ihrerseits waren kürzlich an der internationalen Operation «Golddust» beteiligt, die sich gegen die russische Gruppe REvil richtete. Innert

weniger Monate konnten die Behörden in verschiedenen Ländern mindestens fünf mutmassliche Bandenmitglieder festnehmen.

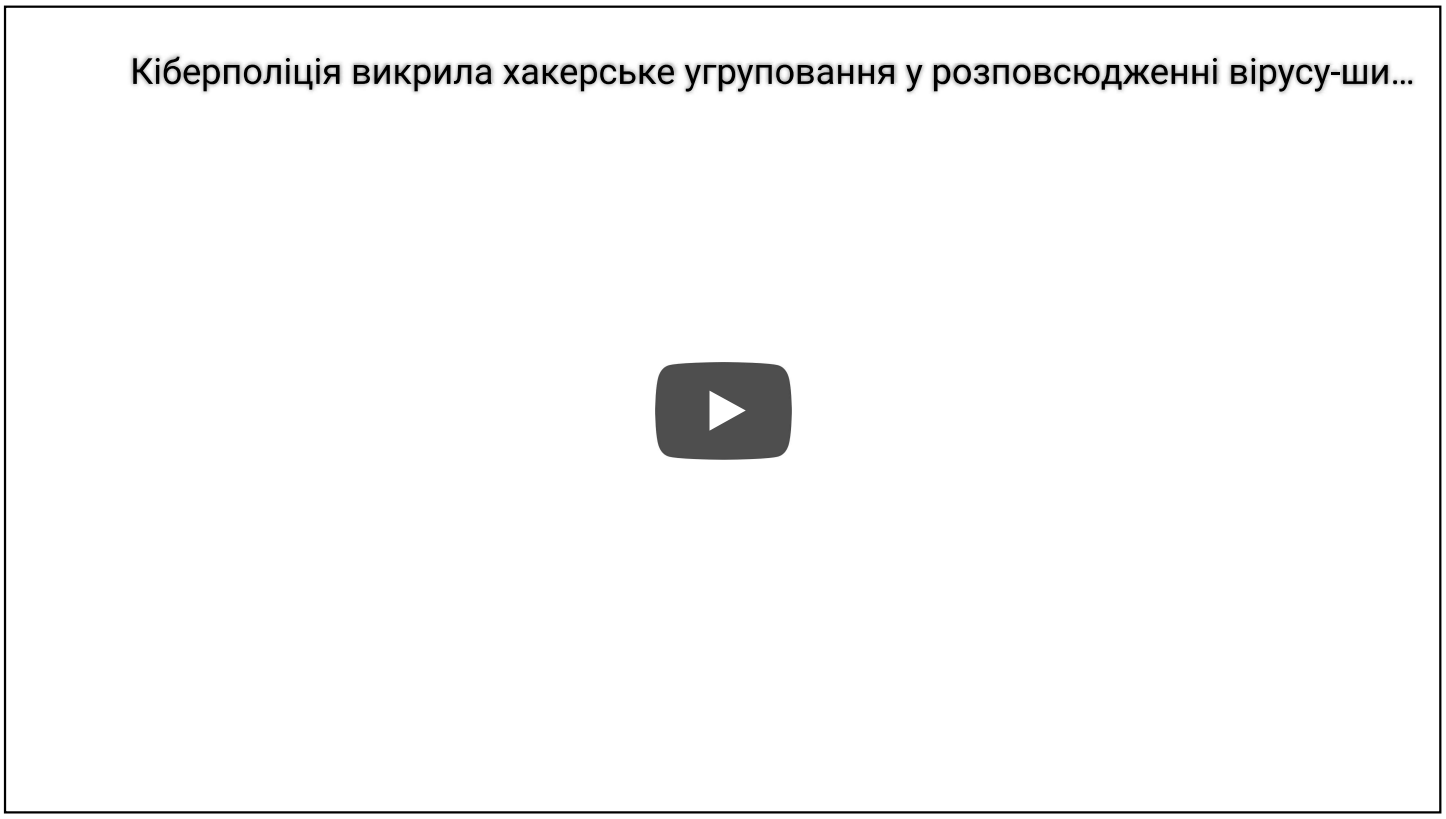


Fahndungsplakat des FBI gegen ein Mitglied der russischen Hackergruppe REvil.
Foto: PD

«Die Strafverfolger mussten ihre Kompetenzen in diesem Bereich zuerst aufbauen. Nun können wir die Früchte davon ernten», sagt Cyber-Ermittler Serdar Günal Rütsche. Laut ihm laufen in der Schweiz aktuell neben dem Basler Fall noch fünf bis zehn weitere Ransomware-Strafverfahren.

Wenn der oberste Schweizer Cyber-Ermittler einen Wunsch hätte, dann wäre es ein Mentalitätswandel. «Tief in vielen Köpfen steckt die Überzeugung: In unserem

Unternehmen passiert schon nichts. Und wenn, dann ist es nicht so schlimm. Das muss sich ändern, wenn Schweizer Firmen nicht mehr so häufig im Visier der Cyber-Kriminellen stehen wollen.»



Bilder einer Interpol-Aktion gegen Ransomware-Cyberkriminelle in Korea und der Ukraine von diesem Sommer.

SonntagsZeitung

Dieser Text stammt aus der aktuellen Ausgabe. Jetzt alle Artikel im E-Paper der SonntagsZeitung lesen: App für iOS – App für Android – Web-App

Publiziert: 04.12.2021, 23:03

Fehler gefunden? Jetzt melden.

THEMEN

Hacking Kriminalität Cyber-Security

7 Kommentare

Ihr Name

Speichern

Sortieren nach: **Neueste**

Willy Kauer
06.12.2021

Besten Dank Herr M. Meier für ihre Wertvolle Infos ich habe ihre Schreiben bei mir gespeichert.

Also habe ich durch sie eine tolle Firma gefunden. Besten Dank für ihre Wertvollen Tipps

Sie kennen logisch Green Datacenter.

Vor rund 24 Jahre lernte ich einen Mann kennen, der wohnte im gleichen Haus, der erzählte von so riesige Datenspeicher, damals war ich tatsächlich so naiv und hatte keine Ahnung davon,

was der Mann so redet.

Nun es ist logisch, dass die meine Webseite entsprechend gesichert wird bei bekannten grossen Fischen. Aber die Sicherheit ist mir viel Wert also komme ich auch zu ihnen.

Nicht desto trotz finde ich eine Absicherung also ein solides Backup und Daten auf dem Papier

für kleinere und mittlere Firmen durchwegs sinnvoll.

1 | 2 | Antworten | Melden

Willy Kauer
05.12.2021

Es ist mir schleierhaft, wieso man Erpresser zahlt, den nur so können sie weitermachen. Wenn niemand zahlen würde, so müssten diese eine Arbeit suchen, wer weiss sogar als

IT-Fachmann.

Ich selbst bin im Aufbau einer grösseren Webseite. Es ist mit sehr viel Arbeit verbunden, es ist doch logisch, dass man im Aufbau alle Sicherheiten ausbauen muss.

Also ein solides Backup sollte doch selbstverständlich sein.

Nicht nur das, darüber hinaus diese Daten in X Orten speichert. Sondern auch auf Blätter alles ausdruckt. Diese dann im Tresor sichert und in externem Miet-Tresor.

Das ist offensichtlich für viele zu viel Arbeit.

Selbstverständlich spezialisierte Firmen hinzuzieht.

Ausserdem Reserve Computer hat, die nicht im System angeschlossen sind.

Darüber hinaus sollte man entsprechende Versicherung haben.

Jeder Laden und Restaurant Besitzer versichert sich ja auch gegen Einbruch.

Als selbständiger Wirt (42 Jahre lang) habe ich immer alles überversichert.

Denn irgendwann gibt es immer einen Schaden. So hat man wenigstens die Kosten

bezahlt.

Bei einigen Betreibungs-Ämter, bei dem man den Auszug für 18.— bestellen kann, bekommt ohne jegliche Absicherung ein Mail mit dem Auszug.

Man könnte es per Post zustellen, was offensichtlich für einige zu aufwendig ist.

Es gibt aber auch inzwischen etliche vorbildliche Firmen, die sich absichern. Ebenso

Zahnärzte und Ärzte, die das Mail absichern mit einem Code.

Oder eben per Post es zustellen.

1 | 3 | Antworten | Melden

M. Meier
06.12.2021

@Willy Kauer
Sie sind ein bisschen naiv, wenn Sie von Tresoren, Ersatzcomputern oder Ausdrucken auf Papier zur Datensicherung reden. Es geht hier nicht um statische Webseiten von ein paar Kilobytes, die man sichern müsste. Es geht vielmehr um dynamische Datenbanken, die viele, viele Terabytes an Daten enthalten, die sich auch noch fortlaufend verändern.

Bei meinem Arbeitgeber sind aktuell rund 500 Gigabyte an Kundendaten gespeichert (Tendenz exponentiell steigend), was im Vergleich zu anderen Firmen nicht einmal besonders viel ist. Wenn Sie das auf Papier ausdrucken wollten, dann ergäbe das rund 250 Millionen bedruckte A4-Seiten! Mit Standard-Papier von 80g pro Seite und doppelseitig bedruckt hätte der Ausdruck ein Gewicht von rund 10'000 Tonnen! Und wenn Sie mit dem Ausdrucken fertig wären, dann könnten Sie gleich wieder von vorne anfangen, da die Daten eben fortlaufend ändern und neue hinzu kommen. Last but not least würde das Wiedereinlesen der Daten von Papier, wenn es denn einmal nötig wäre, wahrscheinlich Monate oder Jahre dauern.

Auch der "Tresor" scheidet aus, weil selbst bei elektronischer Speicherung der Personal- und Zeitaufwand und die Kosten enorm wären, um das alles immer und immer wieder auf physischen Datenträger zu speichern und diese jeweils in einem Tresor zu verwahren.

Kurz: Ihre "grösseren Webseite" mag ja schön und recht sein, aber mit den tatsächlichen Herausforderungen, welche die Datensicherung schon bei relativ "kleinen" Systemen darstellt, hat das nichts zu tun.

2 | | Antworten | Melden

M. Meier
06.12.2021

@Willy Kauer
PS, hier noch ein praktischer Tipp für die Sicherung Ihrer Website: Informieren Sie sich über das Werkzeug namens "Git", welche für die versionierte Speicherung von "Source-Code" dient (also auch dem HTML-Code, der Bilder etc., welche Ihre Website ausmachen).

Wenn Sie gegen geringes Entgelt einen Account bei github.com oder gitlab.com mieten und den Code für Ihre Site mit Git verwalten, ist Ihr Code fast "bombensicher" vor jeglicher Art von Verlust. Einerseits lagern Kopien davon dann sowohl lokal auf Ihrem PC wie auch jederzeit auf dem Server des Git-Providers (und unterliegem dort dem professionellen Backup-Konzept des Providers).

Andererseits erlaubt Git nicht nur die Wiederherstellung der letzten Version des Codes sondern auch aller vorherigen Versionen. Das ist unter anderem bei Ransomware-Erpressern sehr hilfreich. Der Erpresser kann zwar Ihre lokale Kopie verschlüsseln und diese Änderungen auch auf dem Git-Server speichern. Da dort (ausserhalb des Zugriffs des Erpressers) aber auch alle vorherigen Versionen noch gespeichert sind, kann man ganz einfach die letzte "gute" Version des Codes wieder herstellen.

So sichern zumindest wir Profis unseren Source-Code. Für Ihre "grössere Website" (die verglichen mit der Programmierung von ernsthaften Online-Anwendungen wohl eher ein kleines Hobby-Projekt ist 😉) wäre das durchaus auch empfehlenswert, vorausgesetzt Sie können die Zeit aufbringen, zunächst etwas über Git und Source-Code-Verwaltung zu lernen.

^ 1 | v | Antworten | Melden

Willy Kauer
06.12.2021

@M. Meier
Werter Herr Meier, ich gebe zu ich bin schon ein bisschen naiv aber so schlimm ist es auch nicht.

Ich rede hier von kleineren / mittleren Firmen. Sehen sie bei mir wurde 4 mal eingebrochen innert 10 Jahren im Restaurant. Also ein Hacker Angriff könnte ja auch auf klein und mittel Firma betreffen.

Deswegen schlug ich ja Versicherung vor. Klein und Mittelfirmen haben ja nicht so viele Tonnen Papier wie sie es beschreiben.

Aber sehen sie, ich bin wahrscheinlich ein paar Wochen älter als sie.

Die Firma Stadler Rail mit Herr Spuler wurde angegriffen.

Dieselbe Firma hätte 1975 damals ohne Computer auch alles sichern können.

Auch eine Migros oder Coop konnten damals 1975 ohne Computer und Surfer

die Daten sichern. Klar braucht es mehr KV Leute hierfür.

Aber die Erpresser wollen ja auch Geld.

Es muss sicher nicht alles aufs Papier. Aber was wichtig ist halt schon.

Ausserdem kann man alles selbst Speichern auf verschiedene Datenträger und sicher in der Firma aufbewahren.

Externe Datenträger bietet für wenig Geld z.b. Swisscom an.

Hacker Angriff sind nicht nur auf Grossfirmen.

Meine Kommentar ging an klein und Mittelfirma.

Sie reden hier aber von Grossfirmen. Meine Tipps bezieht auf klein und Mittelfirmen.

1 | 1 | Antworten | Melden

M. Meier
06.12.2021

@Willy Kauer
Mein Arbeitgeber hat aktuell ca. 50 Angestellte. Vor 6 Jahren als ich da angefangen habe, waren es sogar noch weniger als 20. Ich würde das (noch) nicht gerade eine "Grossfirma" nennen, auch wenn weiteres Wachstum absehbar ist. 😉

Aber mit 50 Angestellten schreiben und betreiben wir halt Software, welche die Zahlungstransaktionen von einigen zehntausend Online-Shops durchführt. Da kommen Zahlungsdaten von einigen Millionen Endkunden zusammen, bis hin zu jedem einzelnen Produkt, dass diese Kunden in den letzten Jahren bei einem dieser Shops gekauft haben.

Aber lassen Sie sich von den "einigen zehntausend Online-Shops" nicht täuschen! Das ist nicht sehr viel. Wir agieren halt auf einem globalen Markt, und da sind wir nur ein sehr kleiner Fisch in einem Becken voller Haifische, die tausendfach grösser sind. Aber bis jetzt schlagen wir uns ganz gut.

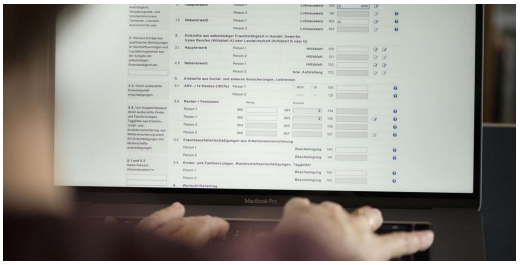
1 | | Antworten | Melden

Sander Steffen
05.12.2021

Herr Günal Rütsche hat schon recht: Als IT-Dienstleister erleben wir immer wieder, dass bei manchen Schweizer KMU keinerlei Investitionsbereitschaft besteht, was die IT-Sicherheit angeht. Die zahlen Jahreslohnsummen in Millionenhöhe, finden aber ein paar Tausend für ein solides Backup sei viel zu teuer und Serverwartungen brauche es sowieso nicht weil "er läuft ja auch ohne und wenn er nicht mehr laufen sollte, können wir euch ja anrufen".

7 | | Antworten | Melden

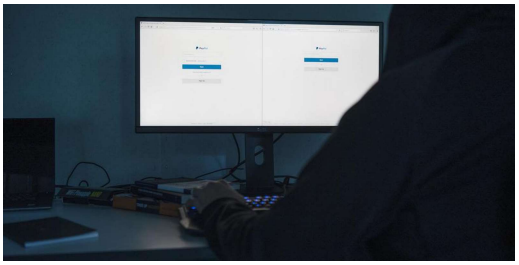
MEHR ZUM THEMA



Internet

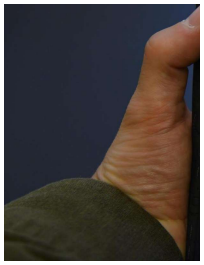
Hochvertrauliche Daten von Privatpersonen und Firmen aus den Kantonen Zürich, Zug und Schwyz sind online zugänglich. Damit erreicht die Cyberkriminalität eine neue Dimension.

09.11.2021



Einem Team aus 17 Nationen ist ein grosser Schlag gegen Hacker gelungen. Die Cyber-Kriminelle sollen für Tausende Attacken auf Organisationen und Firmen verantwortlich sein.

08.11.2021



beantragt hatt
«Hacker» hatte

21.10.2021