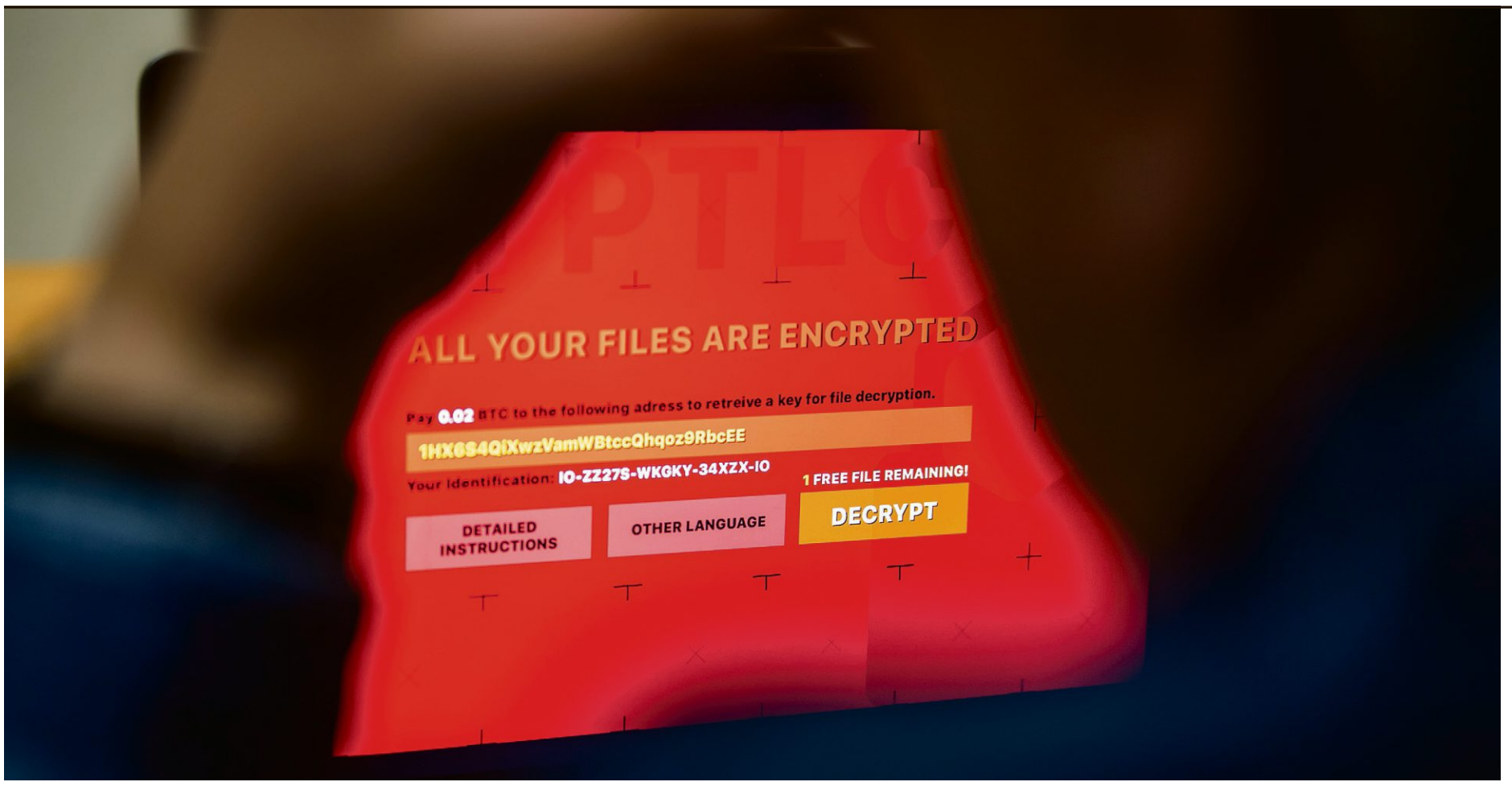


Bei Angriffen mit Erpressungssoftware werden Daten auf Computern verschlüsselt, und die Hacker verlangen Geld für die Freigabe. Foto: Lino Mirgeler (DPA, Keystone)

CEO-Fraud ist die häufigste Angriffsmethode

Angaben in Prozent
■ Betroffene Unternehmen
■ Nicht betroffene Unternehmen

	Betroffene Unternehmen	Nicht betroffene Unternehmen
CEO-Fraud*	49,8	50,2
Phishing	43,1	56,9
Sonstige Schadsoftware	20,7	79,3
Hackerangriff	17,1	82,9
Sonstiges Social Engineering	16,2	83,8
Denial-of-Service-Attacke	11,5	88,5
Ransomwareangriff	11,3	88,7

* Kriminelle geben sich als Mitglied der Geschäftsleitung aus und weisen die Finanzabteilung per E-Mail an, eine Zahlung an sie zu tätigen.

Grafik: luc, mrue / Quelle: Universität Bern

So viele Hackerangriffe wie noch nie

Teures Risiko Rotes Kreuz, Emil Frey, Läderach: 2022 wurden über 34'000 Cyberattacken gemeldet, und die Dunkelziffer ist gross. Das kostet die Wirtschaft bis zu einige Milliarden Franken. Auch die öffentliche Hand ist betroffen.

Simone Luchetta

Erstmals tauchen Cyberattacken im Bericht des Weltwirtschaftsforums (WEF) über die weltweit grössten Risiken unter den Top 10 auf. Sowohl kurz- als auch langfristig halten die 1200 befragten Fachleute und Führungspersonen die Gefahr von Hackerangriffen für hoch (Platz 8).

Auch die Schweiz ist davor nicht gefeit. Das zeigen die jüngsten Zahlen des Nationalen Zentrums für Cybersicherheit des Bundes (NCSC). Im letzten Jahr sind dort rund 34'000 Meldungen zu Cybervorfällen eingegangen – so viele wie nie zuvor, 13'000 mehr als im Vorjahr und dreimal so viele wie 2020.

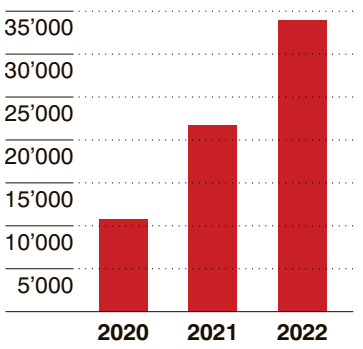
Wie gut ist die Schweiz gegen Cyberrisiken gerüstet? Wer war im vergangenen Jahr besonders betroffen, und was waren die grössten Bedrohungen? Wir haben bei Experten nachgefragt.

— Wie viele Cyberangriffe gab es 2022 in der Schweiz?
Genaue Zahlen gibt es nicht, weil keine Stelle alle Angriffe erfasst. Das NCSC nimmt Meldungen zu sogenannten Cybervorfällen und Schwachstellen von Unternehmen, Verwaltungen und aus der Bevölkerung entgegen. Bei den gemeldeten Vorfällen handelt es sich aber nicht immer um erfolgreiche Cyberangriffe: «Es besteht in der Schweiz keine generelle Meldepflicht. Daher kann die Dunkelziffer entsprechend höher sein», sagt Florian Schütz, Leiter des NCSC. Lediglich rund ein Viertel aller Fälle wird gemeldet, schätzen Sicherheitsexperten.

«Die Angriffe aus dem Cyberraum werden immer professioneller und hochgradig automatisiert ausgeführt», sagt Nicolas Mayencourt, Chef der Cybersicherheitsfirma Dreamlab in Bern. Immer mehr Unternehmen digitalisieren ihre Geschäftsabläufe. Das bietet eine grössere Angriffsfläche. «Hinzu kam 2020 der Cybercrime-Beschleuniger Nummer 1: Covid», so Mayencourt. Gleichzeitig haben immer mehr Menschen Zugang zum Internet, vor allem in Entwicklungsländern. Somit steige auch die Anzahl Menschen, welche das Internet für betrügerische Handlungen und Cyberangriffe verwenden könnten, sagt Roman Hüssy, Gründer der privaten Cyberabwehr-Initiative Abuse.ch.

Cybervorfälle haben in der Schweiz zugenommen

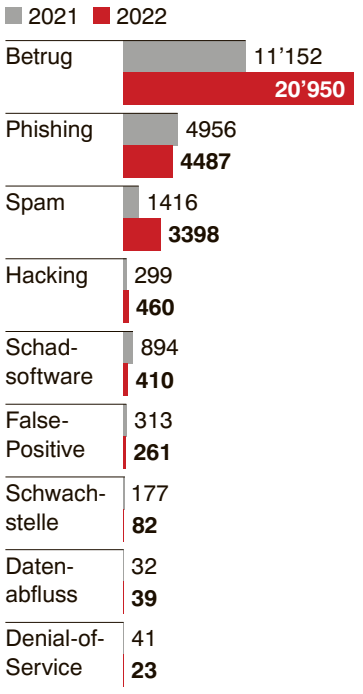
Beim Nationalen Zentrum für Cybersicherheit (NCSC) eingegangene Meldungen



Grafik: luc, mrue / Quelle: NCSC, Stand 21. Dezember 2022

Betrugsmeldungen haben sich 2022 fast verdoppelt

Auswahl gemeldeter Cybervorfälle



Grafik: luc, mrue / Quelle: NCSC

— Wie gut sind in der Schweiz die Heimanwender gegen Cyberangriffe geschützt?
«Das hängt von den einzelnen Personen ab und deren Umgang mit Computer und Internet», erklärt Hüssy. Entscheidend sei, ob die Nutzer Software-Aktualisierungen regelmässig machten und misstrauisch gegenüber verlockenden Finanzangeboten seien. Hüssy: «Viele Leute sind noch immer zu leichtgläubig gegenüber Informationen im Internet.»

Die Verantwortung, sich zu schützen, liegt bei den Heimanwenderinnen und -anwendern. Mayencourt sieht hier auch den Bund in der Pflicht. Viele Menschen arbeiteten seit der Pandemie häufiger im Homeoffice: «Das Privatleben ist also stärker mit dem Arbeitsleben vermischt. Das Problem ist, dass sie von ihren privaten Netzwerken von zu Hause aus auf Firmengeräte zugreifen.»

— Welches waren die häufigsten Angriffsmethoden?
Heimanwender waren 2022 oft Ziel von Betrugsversuchen. Erfolgreich waren und sind Cyberkriminelle mit Fake-Extortion-E-Mails. Dabei handelt es sich um angebliche Drohmails von Strafverfolgungsbehörden. Darin wird behauptet, dass der Empfänger eines massiven Fehlverhaltens – typischerweise in Zusammenhang mit Kinderpornografie – überführt worden sei und die Anklage nur durch eine Geldzahlung fallen gelassen werden könne.

Die Zahl der Betrugsmeldungen insgesamt hat sich 2022 im Vergleich zum Vorjahreszeitraum beinahe verdoppelt:

Das grosse Geld holen Kriminelle aber nicht bei den Heimanwendern. «Der Fokus der organisierten Cyberkriminalität liegt bei Unternehmen, Organisationen und Staaten», sagt Dreamlab-Chef Mayencourt.

— Wo lauern die grössten Gefahren für Unternehmen?
Die häufigste Angriffsform auf Firmen und Institutionen war der sogenannte CEO-Fraud. Das zeigt eine Umfrage des Verbands der Maschinen-, Elektro- und Metallindustrie Swissmem und des Instituts für Strafrecht und Kriminologie der Universität Bern bei den 1200 Mitgliederfirmen. Kriminelle versuchen, beim Finanzverantwortlichen Zahlungen auszulösen, indem sie sich als Chef der Firma ausgeben. Rund die Hälfte der Firmen war davon betroffen.

Die befragten Sicherheitsexperten sehen die grösste Gefahr aber in sogenannten Ransomware-Angriffen. Dabei dringen Angreifer ins Firmen-IT-System ein, stehlen und verschlüsseln Daten und versprechen eine Entschlüsselung erst nach Zahlung eines Lösegeldes (englisch: ransom). Die Cyberfirma Infoguard bearbeitete 2022 über 150 Fälle – gegenüber 120 im Vorjahr. Auch beim NCSC haben die Meldungen von Ransomware-Angriffen seit 2020 (66 Meldungen) deutlich zugenommen. Mit 159 Meldungen sind 2022 aber zwei weniger eingegangen als im Vorjahr.

— Werden auch Mitarbeitende im Homeoffice erpresst?
Ein Drittel der Ransomware-Meldungen betrifft Private. «Erpressungen gegen Heimanwender geschehen heute täglich», sagt Roman Hüssy. So gaukeln Cyberkriminelle dem Heimanwender vor, dass sein Computer gehackt worden sei und man ein delikates Bild und Videomaterial von ihm besitze. Ohne Zahlung eines «Lösegelds» werde das Material im Internet veröffentlicht. Oft verfügten die Kriminellen aber über gar kein kompromittierendes Material, so Hüssy.

— Was soll man bei einem Ransomware-Angriff tun?
«Auf keinen Fall Lösegeld zahlen», rät das NCSC. Es gebe keine Garantie, dass die Verbrecher nach der Lösegeldzahlung die Daten nicht doch noch veröffentlichten. Zudem motiviere jede erfolgreiche Erpressung die Täter zum Weitermachen.

Wollen Opfer dennoch Geld bezahlen, so empfiehlt das NCSC dringend die Kontaktaufnahme mit der Kantonspolizei. Die Website Nomoreransom.org gibt Ratschläge, wie man die Schadsoftware identifizieren kann.

— Welche Angriffe gaben 2022 besonders zu reden?
Einer der grössten Cyberangriffe betraf das Internationale Komitee vom Roten Kreuz. Zu den bekannten Opfern zählten auch der Glarner Schokoladenproduzent Läderach, der Autohändler Emil Frey, die CPH-Papierfabrik in Perlen LU und die Flughafen-Servicegesellschaft Swissport. Dazu gesellen sich die Uni Neuenburg oder die Gemeinde Messen SO. Bei solchen Attacken ist meist nicht nur der Geschäftsbetrieb gestört. Cyberkriminelle entwenden oft auch heikle Daten der Kundschaft, die im Darkweb veröffentlicht oder weiterverkauft werden.

— Sind Schweizer Firmen genug geschützt?
Viele Firmenserver weisen zahlreiche Sicherheitslücken auf – bei Grosskonzernen wie KMU. «Der Zustand ist teilweise katastrophal», sagt Gunnar Porada. Mit seiner Sicherheitsfirma Innosec in Weggis LU klopft er Unternehmen in deren Auftrag nach Schwachstellen auf den Websites ab. «Wir haben kürzlich im Auftrag eines IT-Magazins zwei Detailhändler, eine Bank, ein IT-Unternehmen und einen Branchenverband gescannt. Alle haben schlecht abgeschnitten. Die Lücken waren grösstenteils längst bekannt und hätten von der IT mit einem Update geflickt werden müssen.» Viele Chefs delegierten das Thema Cybersicherheit an die IT-Verantwortlichen, die ihrerseits Sicherheitslücken gern unter den Teppich kehrten, sagt Porada: «Aber Cybersicherheit ist Chefsache.»

— Macht es die öffentliche Hand besser?
«Die Angreifer suchen nach verwundbaren Systemen und greifen diese an, egal ob es sich um eine Verwaltung, ein Spital oder eine Firma handelt», sagt NCSC-Leiter Schütz. Die Websites vieler Gemeinden und Städte weisen zahlreiche Schwachstellen auf. Die Scans von Innosec ergaben etwa für Luzern «erstaunlich gute Resultate», bei Schaffhausen und Zug waren laut Porada die Resultate «eher bestürzend».

Auch in Spitälern registrierte man im letzten Jahr eine Zunahme von Cybervorfällen. Kriminelle nutzten dabei aktuelle Ereignisse wie Corona und den Lockdown: «Organisationen, die sowieso schon unter Druck sind, können dann effektiver erpresst werden», sagt Schütz. Dabei können personenbezogene Daten für Identitätsdiebstahl missbraucht werden. Betroffene müssen in der Folge oftmals ein Leben lang immer wieder beweisen, dass sie ein Verbrechen oder eine Tat nicht begangen haben.

— Wie gross ist der wirtschaftliche Schaden durch Cyberdelikte?
Schätzungen für 2022 gehen von mehr als 6 Billionen Franken weltweit aus. Bis 2025 soll der globale Schaden bei über 10 Billionen Franken liegen. «In der Schweiz wird der wirtschaftliche Schaden auf bis zu einige Milliarden Franken geschätzt», sagt Thomas Meyer von Infoguard.