



CYBER- SECURITY:

Sicherheit im Cyberspace

CYBER- SECURITY

Das Internet vernetzt uns mit der ganzen Welt. Es ist eine Welt voll von spannendem Wissen und Unterhaltung. Kurz:

Der Cyberspace ist supercool. Aber wer sich im digitalen Raum bewegt, setzt sich auch gewissen Gefahren aus. Denn Ver-

netzung ist keine Einbahnstrasse. Sie gibt nicht nur uns Zugang zur Welt, sondern auch der Welt Zugang zu uns. Das nutzen

Cyberkriminelle aus: Sie suchen Schlupflöcher, durch die sie in Informatiksysteme eindringen und an sensible Daten gelangen

können. Kein Grund zur Panik, aber Grund genug, um

möglichst cybersmart zu sein. Denn nur wer die Risiken kennt,

fällt auf die fiesen Tricks der Cyberverbrecher nicht herein.

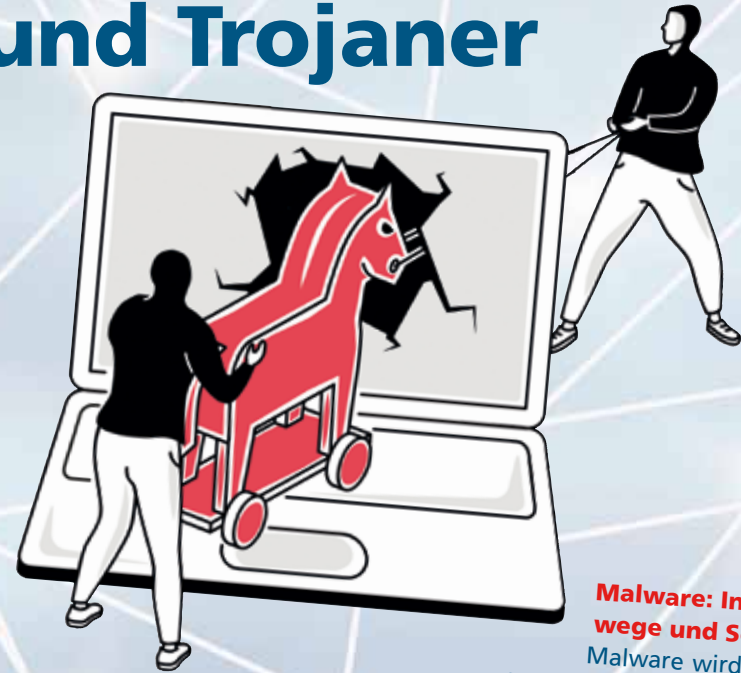
Was Hacker wollen

Cyberangriffe zielen darauf ab, Daten und Informationen zu stehlen, zu verändern oder zu zerstören – und daraus Profit zu schlagen. Mit den erbeuteten Informationen können Datendiebe entweder direkt auf Kreditkarten und Bankkonten zugreifen oder sie können Menschen erpressen, damit sie ihnen Geld überweisen. Sie können Identitäten klauen und im Namen und auf Kosten ihrer Opfer online einkaufen oder massenhaft Spam verschicken, um an wertvolle Daten zu gelangen. Und schliesslich können sie die gestohlenen Daten im Darknet – dem Teil des Internets, der nicht über herkömmliche Suchmaschinen oder Browser zugänglich ist – an andere Kriminelle weiterverkaufen.



Spionage und Manipulation: Solche Angriffe fügen Unternehmen, Behörden und auch Einzelpersonen grossen Schaden zu. Oft richten sie sich auch gegen kritische Infrastrukturen. Dann fällt zum Beispiel die Stromversorgung aus oder Spitäler werden tagelang lahmgelegt – mit schwerwiegenden Folgen für die Patient:innen. Nicht immer geht es dabei um Geld: Hinter Cyberattacken stehen manchmal auch verfeindete Staaten, die sich gegenseitig fleissig ausspionieren oder versuchen, Wahlen zu manipulieren.

Böse Schädlinge: Viren, Würmer und Trojaner



Malware ist der Oberbegriff für schädliche Computerprogramme. Dazu gehören Viren (verstecken sich häufig in Anhängen und werden aktiv, sobald diese geöffnet werden), Würmer (verbreiten sich von selbst) und Trojaner (tarnen sich als hilfreiche Programme). Exploits spüren Sicherheitslücken auf und nutzen sie, um schädlichen Code zu platzieren: Das gelingt am besten, wenn die Software nicht auf dem neusten Stand ist. Keylogger lesen heimlich mit und registrieren alles, was auf der Tastatur eingetippt wird.

Malware: Infektionswege und Schäden

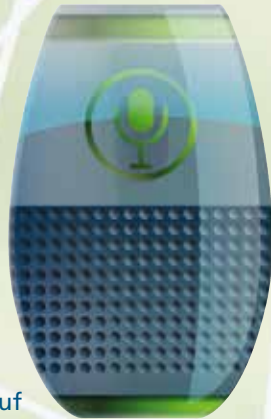
Malware wird über E-Mail-Anhänge, Downloads, manipulierte Websites, USB-Sticks oder fragwürdige Links in Systeme eingeschleust. Dort spioniert sie Daten aus, löscht oder verschlüsselt Dateien und legt ganze Netzwerke lahm.

Ransomware: Erpressung durch Datenverschlüsselung

Besonders perfid ist Ransomware: Hier sperren die Angreifer Dateien oder schalten ganze Systeme aus und verlangen dann Lösegeld, um sie wieder freizugeben. Wer nicht zahlt, dessen Daten werden im Darknet veröffentlicht.

Wo Cybergefahren lauern

Technische Schwachstellen



Alexa hört mit:

Smarte Lautsprecher, intelligente Lichtschalter, Staubsaugerroboter, Fitnessstracker – immer mehr elektronische Geräte sind mit dem Internet verbunden und sammeln Daten. Beim Kauf schauen wir darauf, was so ein Gerät kann, was es kostet und ob sein Design uns zusagt. Darüber, was für Daten es speichert und wer darauf Zugriff hat, machen wir uns hingegen kaum Gedanken. Selbst Autos sind heute datensammelnde Computer auf Rädern. Das macht sie – wie alle mit dem Internet verbundenen Geräte – verwundbar für Hacker-Angriffe.

Offline und trotzdem gefährlich:

Auch in USB-Sticks und externen Festplatten kann Malware schlummern.



Elektronische Schwachstellen



UPDATE



Lästig, aber unverzichtbar:

Hinweise auf Updates nerven und sind schnell weggeklickt. Doch ohne diese verbesserten oder korrigierten Software-Versionen sind Betriebssysteme und Apps bald veraltet. Unentbehrlich sind auch eine Firewall, die den Computer gegen Angriffe von aussen schützt, und Virenschutzprogramme, die Malware erkennen und blockieren.

Tipps: So bewegt man sich im Cyberraum sicher



Updates und Backups:

Software-Updates regelmäßig und zeitnah ausführen und auch regelmäßig ein Backup, d. h. eine Kopie aller wichtigen Daten, auf einer externen Festplatte oder einem USB-Stick erstellen (und sicher aufbewahren).



Kritisch sein und im Zweifelsfall löschen:

Keine Links in E-Mails, SMS, Social-Media-Posts etc. anklicken und keine PDFs öffnen, deren Absender:in man nicht kennt. Stattdessen: löschen! Auch wenn so ab und zu eine echte Nachricht im Mülleimer landet – wenn es wichtig war, werden sich die Absender:innen sicher nochmals melden.

Organisatorische Schwachstelle



Nie ohne Backup: Nicht gesicherte Daten, die gestohlen werden, sind für immer weg. Fehlende Zugangsbeschränkungen sind eine Barriere weniger für Eindringlinge, dasselbe gilt für schwache Passwörter. Riskant ist es auch, wenn Angestellte ihre eigenen Laptops oder Tablets mit zur Arbeit bringen und dann sensible Geschäftsdaten auf demselben Gerät bearbeiten, auf dem sie auch auf unsicheren Websites surfen.

Physische Schwachstellen

Hände weg: Liegen meine Geräte unbeaufsichtigt herum? Können vermeintliche Handwerker:innen einfach in ein Unternehmen hineinspazieren? Sind die Bildschirme in den Büros gesperrt oder jedem und jeder frei zugänglich?



Die grösste Risikoquelle: Der Faktor Mensch

Cyberkriminelle wissen, dass Menschen leichter zu knacken sind als ausgeklügelte Sicherheitssysteme. **Social-Engineering-Attacken** manipulieren menschliche Eigenschaften wie Gutgläubigkeit, Hilfsbereitschaft und Respekt vor Autoritäten ganz gezielt, um an vertrauliche Informationen zu gelangen. Beim so genannten CEO-Fraud zum Beispiel geben sie sich als Chef:in eines Unternehmens aus, machen psychologischen Stress und verlangen eine sofortige Geldüberweisung. In Hongkong ist ein Unternehmen Anfang dieses Jahres so um 22 Millionen Franken betrogen worden.



Persönliches für sich behalten:

Keine persönlichen oder sensiblen Informationen mit unbekanntem Personen teilen, weder per E-Mail noch per SMS, WhatsApp, in Chaträumen, auf Social-Media-Plattformen oder am Telefon. Handys, Tablets und Laptops nicht unbeaufsichtigt herumliegen lassen oder Fremden ausleihen. Keine fremden Powerbanks und USB-Sticks nutzen. Und Gratis-WiFi nur, wenn es nicht um sensible Daten geht.



Starke Passwörter nutzen:

mindestens 12 Zeichen lang, mit Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen. Ein Passwort-Manager hilft, Passwörter sicher zu speichern und den Überblick nicht zu verlieren. Wenn immer möglich den Passwortschutz durch die Zwei-Faktor-Authentifizierung ergänzen.



Beim **Phishing** (password fishing) werden die Opfer mit betrügerischen, aber täuschend echt aussehenden E-Mails dazu verleitet, vertrauliche Informationen preiszugeben oder auf einen Link zu klicken und so Malware herunterzuladen.

Im Internet ist eine grosse Portion Misstrauen angebracht. Was zu gut klingt, um wahr zu sein, ist es meist auch nicht: E-Mails, die uns einen Gewinn oder eine Erbschaft vorgaukeln, sind mit Sicherheit üble Tricks. **Gratis-WLAN** ist oft schlecht geschützt (also eher nicht fürs E-Banking geeignet). **Apps** mögen kostenlos sein, haben dafür aber oft Zugriff auf persönliche Daten wie Kontakte oder Anruflisten. Und manche Verkaufsportale, die spottgünstig Designer-Klamotten oder Qualitätsfahrräder anbieten, sind ganz einfach **Fake-Shops**.



«**Schutztruppen**» mobilisieren: Virenschutzprogramm und Firewall im Betriebssystem aktivieren und mit automatischen Updates auf dem neusten Stand halten.

berufsberatung.ch



Nadine Bless
Studien- und Laufbahnberaterin
BSLB St.Gallen

Wünschst du Unterstützung in der Berufs- oder Studienwahl? Oder mehr Informationen zu den einzelnen Berufsbildern? Dann melde dich bei der Berufs- oder Studienberatung in deinem Kanton. Hier findest du alle Adressen der Berufsberatungsstellen:
BIZ - berufsberatung.ch

Wie wirst du Cyber-Security-Expert:in?
Viele Wege führen nach Rom – so auch in diesem Feld. Ob über eine berufliche Grundbildung, als Informatiker:in oder Elektroniker:in und späterer Weiterbildung oder über eine Berufs-/gymnasiale Matura mit einem Hochschulstudium: Spezialist:innen in diesem Bereich sind sehr gefragt auf dem Arbeitsmarkt. Diese grosse Nachfrage führt auch zu neuen Ausbildungen, Studienrichtungen und Berufen, wie z. B. zum/r ICT-Security-Operations-Manager:in oder zur Berufsprüfung als Cyber Security Specialist. Neben schweizerischen Bildungsangeboten sind internationale Spezialisierungen und Zertifizierungen die Basis für eine Karriere im Bereich Cybersecurity.

«In Cybersecurity erwartest dich jeden Tag etwas Neues. Du arbeitest mit Leuten weltweit und schützt Firmen. Deine Fähigkeiten sind gefragt wie nie. Hier hast du die Chance auf Abenteuer und kannst wirklich was bewegen. Cyber hält dich wach und motiviert – genau das Richtige, wenn du auf Herausforderungen stehst!»
Patrik Bless, Chief Information Security Officer bei Partners Group

Fachkräftemangel in der IT-Branche
Der breite Zugang zur künstlichen Intelligenz (KI) hat die Welt auf den Kopf gestellt. Wir stehen vor der Frage: Wer wird in Zukunft die neuen Technologien effektiver zu seinem Vorteil nutzen – wir oder die Cyberkriminellen? Informiere dich, trage zu einem sicheren Umgang bei, und wer weiss, vielleicht bist du eine/r der Cyber-Security-Spezialist:innen der Zukunft.

Neuer Bachelor an der Hochschule Luzern (HSLU)
Der neue Studiengang in Information & Cyber Security der HSLU vermittelt das notwendige Fachwissen, um sichere IT-Infrastrukturen zu entwickeln und zu betreiben. Studierende lernen im Studium den Umgang mit sensiblen Daten sowie Produkt- und Prozessgeheimnissen und sind in der Lage, Unternehmen und Institutionen aus dem öffentlichen Sektor beim Schutz kritischer Infrastrukturen zu unterstützen. www.hslu.ch > Studium > Bachelor

«Am besten, es kommt gar nicht erst zu einem Cyberangriff»

Seit über 30 Jahren
bekämpft Chris Eckert
Kriminalität. Früher
als Fahndungschef bei
der Kantonspolizei Zürich
und Kommissariatsleiter
der Bundeskriminalpolizei,
heute im Cyberspace.



Technoscope: Was macht ein Cybersecurity-Spezialist?

Chris Eckert: Alle Informatiksysteme – Computer, Server, Datenträger – und alle Kommunikationssysteme – Telefon- und Mobilfunknetze oder WLAN – können angegriffen werden. Wir finden und schliessen technische und organisatorische Schwachstellen und versuchen, das Bewusstsein unserer Kund:innen für Cyberrisiken zu stärken. Denn im Idealfall sollte es gar nicht erst zu einem Angriff kommen.

Lässt sich dieses Ideal erreichen?

Leider nein. Cybersicherheitsexpert:innen haben deshalb vor allem mit den Auswirkungen von Cyberangriffen zu tun: Wie kam es zur Attacke, kann man sie stoppen oder den Schaden begrenzen? Wer steckt dahinter, sind

weitere Angriffe zu befürchten und wie sollte ich mich gezielt schützen?

Wer sind Ihre Kunden?

Wir beraten Unternehmen, Privatpersonen und öffentliche Verwaltungen. Manche ziehen es vor, die Sicherheit ganz den Expert:innen zu überlassen.

Ist das nicht riskant? Denn dann meint man vielleicht, selbst nicht mehr aufpassen zu müssen?

Das ist generell ein Problem. Cybersicherheit wird noch zu oft als lästig empfunden. Unter dem Vorwand, nichts von IT zu verstehen, tun viele so, als ginge sie das Problem nichts an, oder schieben es auf andere ab.

Aber Sicherheit ist kein Produkt, das man kauft, und dann ist die Sache erledigt – sie ist ein kontinuierlicher Prozess.

Unterscheiden sich die Risiken für Unternehmen und Privatpersonen?

Die Einfallstore sind dieselben. Bei privaten Smartphones und Tablets sind vor allem die unzähligen Apps und der Umgang damit riskant. Klar, die sind (meist) nützlich, einfach zu bedienen und machen Spass. Aber wir fragen uns viel zu wenig, was mit den Daten passiert, die wir da ständig irgendwohin übermitteln und damit nicht mehr unter Kontrolle haben.

Ist es nicht unrealistisch zu verlangen, dass Normalnutzer:innen sich bei jeder App genau über solche Dinge informieren?

Wir müssen dringend umdenken und davon wegkommen, kopflos alles Mögliche herunterzuladen. Oder uns völlig bedenkenlos in den sozialen Medien zu bewegen und zu meinen, jede Minute unseres Lebens mit ganz vielen teilen zu müssen. Es ist wie beim Strassenverkehr: Der ist viel sicherer geworden, seit alle Verkehrsteilnehmer:innen bereits in jungen Jahren die Verkehrsregeln lernen und eine Fahrprüfung ablegen müssen.

Wie merkt man, dass man gehackt wurde?

Eigentlich erst, wenn es zu spät ist, der Schaden sichtbar wird oder man erpresst wird. Im Durchschnitt sind Unternehmen bereits vier Monate lang ausspioniert worden,

bevor der Angriff erfolgt. Datendiebe bereiten sich präzise vor, um dann in möglichst kurzer Zeit mit grösstmöglicher Wirkung zuschlagen zu können.

Soll man mit Hackern verhandeln?

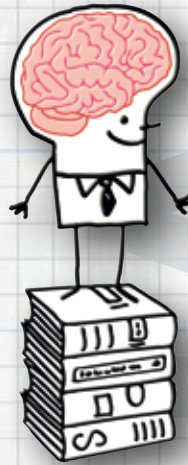
Verhandeln ist grundsätzlich immer besser als die «Türe zuknallen», sonst hat man gar nichts in der Hand. Das gilt in allen Lebenslagen. Man sollte aber mit den so genannten Ransomware-Erpresser:innen nicht selbst verhandeln, sondern dies erfahrenen Expert:innen in Auftrag geben. Dies setzt aber auch voraus, dass man sich frühzeitig Gedanken über die eigene Strategie und Taktik in einem solchen Fall gemacht hat und ein bereits vorbereitetes Sicherheitsdispositiv wirken lassen kann.

Wie wird man Cybersicherheits-expert:in?

Man lernt einen technischen Beruf wie Elektroniker:in, Mediamatiker:in oder Informatiker:in oder studiert in eine solche Richtung, macht Praktika bei verschiedenen Firmen, absolviert Weiterbildungen vor allem auch im Sicherheits- und Risikobereich und sammelt Berufserfahrung im In- und Ausland. Und man spezialisiert sich: Der Informatik- und Elektronikbereich ist so vielfältig, dass man ihn unmöglich komplett abdecken kann. Auch Sprachen sind wichtig: Zumindest Englisch sollte man verhandlungssicher beherrschen. Und schliesslich braucht es Interesse an der weltpolitischen Lage. Denn Cyberangriffe sind immer eng mit der Aktualität verbunden – das macht diesen Beruf auch so spannend.

**Cybersicherheit
wird noch zu oft
als lästig
empfunden.**

So verläuft ein Phishing-Angriff



- 1** Pling! Eine neue E-Mail ist im Postfach. Der Absender scheint seriös: Vielleicht ist es der Paketdienst, der meldet, dass es bei der Zustellung ein Problem gibt; oder die Bank, die ein neues Passwort fürs E-Banking verlangt. Es geht jedenfalls um etwas Wichtiges und das Ganze ist sehr dringend.
- 2** Also rasch den beigefügten Link anklicken ...
- 3** Der Link führt auf die Website des Absenders – dass es eine Kopie der echten Website ist, sieht man ihr nicht an.
- 4** Hier soll man nun ein Formular ausfüllen und alle möglichen persönlichen Daten angeben: Name, Vorname, E-Mail-Adresse, Benutzername und Passwörter für diverse Konten etc.
- 5** Formular abschickt? **Grosser Fehler!**
- 6** Mit den angegebenen Informationen können die Cyberkriminellen nun im Namen des Opfers auftreten, Banküberweisungen tätigen oder online auf dessen Kosten einkaufen.



Cyberangriffe in Zahlen: Ransomware und Phishing auf dem Vormarsch



Durchschnittlich **alle 11 Sekunden** greifen Cyberattacker ein Schweizer Unternehmen oder Organisationen an.



2022 wurden in der Schweiz **34'000 Fälle gemeldet**; jedes dritte KMU war betroffen.

Zu den Opfern gehörten 2022 auch das **Internationale Rote Kreuz**, der grösste Schweizer Autohändler und verschiedene Gemeindeverwaltungen.



Fast jede **zweite Cyberattacke** hing 2021 mit Ransomware zusammen.



Etwa **jede dritte unerwünschte E-Mail** ist ein Phishing-Versuch.



Die Angriffe verursachen grosse Schäden: Expert:innen schätzen, dass die Summe 2025 **weltweit 10'000 Milliarden Franken** übersteigen wird.

Impressum

SATW Technoscope 01/25 | www.satw.ch/technoscope

Konzept und Redaktion: Ester Elices | Redaktionelle Mitarbeit: Christine D'Anna-Huber | Grafik: Andy Braun | Bilder: Adobe Stock | Titelbild: Adobe Stock | Übersetzung und Lektorat: Belinda Weidmann, weiss traductions genossenschaft | Druck: Egger AG

Gratisabonnement und Nachbestellungen

SATW | St. Annagasse 18 | CH-8001 Zürich | technoscope@satw.ch | Tel +41 44 226 50 11

Das nächste Technoscope erscheint im April zum Thema «Textiltechnologien».

satw technology
for society

Gerne können Sie einzelne Exemplare oder einen Klassensatz für Ihre Schulklasse gratis bestellen. Schreiben Sie uns auf technoscope@satw.ch. Alle Ausgaben des Technoscope finden Sie unter satw.ch/technoscope.