next

EIN BLICK IN DIE ZUKUNFT:
CYBERKRIMINALITÄT

*IN DER RUBRIK «NEXT» BELEUCHTEN WIR WICHTIGE THEMEN VON MORGEN.

GLOBALE PERSPEKTIVEN

GRÖSSTE DATENKRAKEN
Die US-amerikanischen Unternehmen Google und Meta sammeln und horten am meisten Daten von Privatpersonen. Dabei besteht wenig Transparenz.

ERSTER CYBERANGRIFF
1834 verschafften sich Kriminelle in Frankreich Zugang zum französischen Telegrafensystem und stahlen so Finanzmarktinformationen. Es war der erste Cyberangriff überhaupt.

SICHERSTES LAND
Polen belegt den ersten Platz im nationalen Cybersicherheitsranking (NCSI), das für verschiedene Staaten erhoben wird. Die meisten Cyberangriffe kommen übrigens aus Russland.

CYBERKRIMINALITÄT
HACKER BEDROHEN DIE GESELLSCHAFT

Cyberkriminelle machen heute mehr Geld als Drogendealer: Schätzungen beziffern den jährlichen Umsatz auf bis zu 1500 Milliarden Dollar. Ziel der Cyber-Attacken sind vor allem Unternehmen und staatliche Institutionen, teilweise auch Privatpersonen. Klassiker sind Ransomware-Angriffe. Dabei verschlüsseln Kriminelle mit spezieller Software die Daten des Opfers und verlangen ein Lösegeld, um sie wieder freizugeben. Ransomware ist im Internet frei käuflich, die dahintersteckenden Firmen sitzen in Drittstaaten, wo sie geduldet oder gar gedeckt werden.

«CYBERKRIMINELLE SIND ORGANISIERT WIE EIN UNTERNEHMEN»*

Wie gehen Internetbetrüger vor? Und wie können wir uns vor ihnen schützen? Die beiden Cybersicherheits-Spezialisten Philipp Leo (links) und Dr. Fabian Muhly (rechts) geben Auskunft.

INTERVIEW—**RAPHAEL HEGGLIN**

«VIELE FÄLLE VON CYBERKRIMINALITÄT WERDEN HEUTE NICHT ZUR ANZEIGE GEBRACHT.»

→ **In der Schweiz kommt es laut Bundesamt für Statistik jeden Tag zu etwa 100 Fällen von Cyberkriminalität. Was sind das für Delikte und wie gehen Cyberkriminelle vor?**

Zuerst etwas zur genannten Zahl: Diese widerspiegelt lediglich die gemeldeten Fälle, die Opferzahl ist in Realität wesentlich höher und dürfte in Zukunft weiter ansteigen. Das liegt daran, dass heute vieles gar nicht zur Anzeige gebracht wird. Denn oft handelt es sich um Kleinbeträge, für die sich der Aufwand nicht lohnt. Oder das Opfer wird mit etwas erpresst, das ihm peinlich ist. Das kann zum Beispiel ein kompromittierendes Foto sein oder der Beleg für eine Sexdienstleistung. Was vielen Menschen nicht bewusst ist: Die meisten Cyberkriminellen gehen hochprofessionell vor und sind organisiert wie ein Unternehmen. Sie wissen oft sehr genau, wieviel sie von jemandem erpressen können, und passen den Aufwand entsprechend an.

Es geht also vielfach um Erpressung?

Ja, bei einer grossen Zahl der Fälle geht es um Erpressung. Diese kann auf verschiedene Arten ablaufen. Sehr häufig ist zum Beispiel der Weg über eine Ransomware. Das ist ein Programm, welches Daten auf einem Computer oder auf einer Datenbank verschlüsselt, womit die Besitzer keinen Zugriff →

*PHILIPP LEO ist Berater zahlreicher Behörden und Organisationen im In- und Ausland und ausgewiesener Experte für Cyberrisiken und Digitalisierung.

*FABIAN MUHLY ist Doktor der Kriminologie und Berater sowie Forscher in der Informationssicherheit. Zusammen betreiben sie die Firma Leo&Muhly, die sich auf Cybersicherheit spezialisiert hat.

LEO&MUHLY
CYBER ADVISORY

FOTOS: ZVG, CLIFF HANG/PIXABAY.COM

next

EIN BLICK IN DIE ZUKUNFT: CYBERKRIMINALITÄT

DIGITALE ETHIK

SCHWEIZ WIRD STANDARDS SETZEN

Die Swiss Digital Initiative (SDI) will Unternehmen weltweit zu verbindlichen ethischen Verhaltensregeln bewegen und mehr Transparenz bei der Datennutzung schaffen. Trägerin der SDI ist die privatrechtlich organisierte Stiftung Swiss Digital Initiative mit Sitz in Genf und wird präsidiert von alt Bundesrätin Doris Leuthard.

LOCKBIT

ORGANISIERTE CYBERKRIMINALITÄT

Die russische Organisation Lockbit gilt als eine der grössten Anbieterinnen von Ransomware. Mit dieser Schadsoftware lassen sich Computer sperren und Daten verschlüsseln. Ransomware ist frei käuflich und für einen grossen Teil der Cyberkriminalität verantwortlich. Im Februar 2024 haben die National Crime Agency, das FBI und Europol gemeldet, dass sie Lockbit zerschlagen haben. Die russischen Drahtzieher gaben jedoch bekannt, sämtliche ihrer Software auf Backupservern gesichert zu haben und weiterhin im Geschäft zu sein.

INTERNETPOLIZEI

EUROPÄISCHES NETZWERK

Vergangenes Jahr hat die Europäische Union das International Cyber Offender Prevention Network (InterCOP) gegründet. Es ist Teil von Europol und dient dem Ziel, die Cyberkriminalität einzudämmen. Denn da Cyberkriminalität international agiert, lässt sie sich nur durch internationale Zusammenarbeit effektiv bekämpfen. InterCOP will einerseits Präventivmassnahmen entwickeln und andererseits die länderübergreifende Strafverfolgung erleichtern. Momentan leitet die Niederlande das Projekt, insgesamt sind 26 Länder daran beteiligt. Zwischen der Schweiz und Europol besteht seit 2006 ein Kooperationsabkommen. Dazu hat das Bundesamt für Polizei fedpol vier Polizeiattachés und das Bundesamt für Zoll und Grenzsicherheit (BAZG) einen Polizeiattaché in Den Haag stationiert.

«SCHON HEUTE LASSEN SICH STIMMEN DURCH KÜNSTLICHE INTELLIGENZ TÄUSCHEND ECHT NACHAHMEN.»

PHILIPP LEO UND DR. FABIAN MUHLY

mehr darauf haben. Die Cyberkriminellen verlangen dann ein Lösegeld, um die Daten wieder freizugeben. Oder sie drohen damit, sensible Daten zu veröffentlichen. Für letzteres werden gehackte Datenbanken systematisch durchsucht, zum Beispiel auf Bilder, Finanz- oder Gesundheitsdaten. Es gibt kriminelle Organisationen, die sich auf Unternehmen und Institutionen spezialisiert haben und jeden einzelnen Angriff akribisch durchplanen. Und dann gibt es solche, die nach dem Giesskannenprinzip arbeiten und versuchen, möglichst viele Privatpersonen um Kleinbeträge zu erleichtern.

Damit dies gelingt, muss also zuerst ein Schadprogramm auf dem Computer installiert werden.

Man glaubt gar nicht, wie raffiniert einige dabei vorgehen. Wir alle kennen diese teilweise plumpen E-Mails mit Post-Ankündigungen oder etwas anderem, bei dem man einen Link anklicken soll. Doch vieles läuft wesentlich subtiler ab, beispielsweise über vertrauenswürdig erscheinende Websites oder Apps, die wir herunterladen. Geht es um grosse Beträge, dann nehmen Cyberkriminelle auch gezielt einzelne Schlüsselpersonen ins Visier und bauen ein Vertrauensverhältnis auf. Dieses sogenannte Social Engineering kann über Wochen und Monate andauern, bis das Ziel erreicht ist – also die Ransomware heruntergeladen wurde. Das muss nicht zwingend über einen Link oder einen direkten Daten-Download ablaufen. Schadware lässt sich zum Beispiel auch über Computerschnittstellen wie USB einbringen. Jemand steckt einen präparierten Ventilator oder ein anderes Computer-Gadget ein und schon ist es passiert …

Mit künstlicher Intelligenz dürften noch mehr Einfallstore entstehen?

Das ist so. Schon heute lassen sich Stimmen synthetisieren, d.h. nachahmen, dass man es nicht merkt. Es reicht dazu eine kurze Originalaufzeichnung der Stimme. Was passiert dann, wenn der so vorgetäuschte Chef anruft und einen zu einer bestimmten Aktion auffordert? Zum Beispiel das soeben gemailte Dossier anzuschauen, welches in Realität ein Schadprogramm ist. Auch Deepfakes mit Foto und Video werden in Zukunft immer ausgeklügelter sein. Anfang April berichtete das Bundesamt für Cybersicherheit über den ersten Angriff auf ein schweizerisches Unternehmen, bei dem Stimme und Erscheinungsbild des vermeintlichen CEOs in einer manipulierten Videokonferenz Deepfake waren. Interviews, Videokonferenzen und vieles mehr lassen sich also zunehmend fälschen. Sogar Wahlen könnte man auf diese Weise manipulieren. Sorgen bereiten uns zudem Chatbots. Das sind KI-basierte Programme, die Konversation führen können – auch sie funktionieren immer besser. Phishing-Mails lassen sich so künftig durch eine Hotline ergänzen. Wer anruft, weil er misstrauisch wurde, wird automatisch beruhigt. Da es intelligente Sprach-Programme sind, lassen sie sich grossflächig und in grosser Zahl einsetzen.

Cyberkriminelle setzen also vielfach neuste Technologie ein, die Laien nicht verstehen. Wie schützt sich jemand, der kein Computerprofi ist?

Die meisten Privatpersonen sind glücklicherweise nicht so interessant, dass Cyberkriminelle einen grossen Aufwand betreiben würden. Es geht immer um das Kosten-Nutzen-Verhältnis. Das heisst, die Bedrohung besteht in erster Linie aus Viren und Massen-Phishing. Einfache Schutzprogramme wie Virenscanner schützen gut vor solchen Attacken. Sie können es jedoch nur, wenn man regelmässig ein Update macht – was leider oft nicht der Fall ist. Zusätzlich empfehlen wir regelmässige Datenbackups auf passwortgeschützte Datenträger wie eine externe Festplatte. Auch dazu reichen Standardprodukte. Von wichtigen Daten sollte man drei Backups haben, zum Beispiel auf dem Computer, einem Datenträger und in einer Cloud. Mindestens ein Backup sollte örtlich von den anderen getrennt sein, ansonsten kann ein Hausbrand, ein Wasserschaden oder ein anderes Ereignis alles vernichten. Passwortschutz ist ebenfalls wichtig: Passwörter lassen sich in einem Passwort-Safe speichern. So klappt es auch mit zahlreichen Passwörtern, denn eines für alles, das ist heute schlicht viel zu gefährlich.

Auch Privatpersonen können sich also vor Cyberkriminalität schützen?

Ja, es gibt viele Produkte, die effektiv schützen und sich einfach bedienen lassen – dazu muss man kein Nerd sein. Doch nutzen sollte man sie! Und es ist wichtig, dass wir uns alle mit dem Thema beschäftigen, denn Cyberkriminalität wird nicht mehr verschwinden, sie wird sogar noch zunehmen. Genauso selbstverständlich wie das Abschliessen der eigenen Wohnung sollte daher der Schutz der eigenen Daten sein. ●

far away

SCHWEIZ

NEUES DATENSCHUTZ-GESETZ

Seit dem 1. September 2023 ist in der Schweiz das neue Datenschutzgesetz (DSG) in Kraft. Es betrifft alle Firmen und Organisationen, welche Personendaten sammeln und speichern. Neu muss zum Beispiel die Datensicherheit nachweislich durch technische und organisatorische Massnahmen sicherstellen sein, um Cyberangriffe zu verhindern.
Das DSG ist an die europäische Datenschutzgrundverordnung (DSGVO) angelehnt.

CREEPER

AUSSER KONTROLLE GERATEN

Unter dem Namen «Creeper» startete 1971 das erste Projekt, mit dem man die Sicherheit von Computernetzwerken überprüfen wollte. Dazu entwickelte der US-amerikanische Programmierer Bob Thomas einen Computerwurm, der rein experimentellen Zwecken dienen sollte. Unglücklicherweise verselbständigte er sich und befiel das bestehende Netzwerk ARPANET tatsächlich.

FOTOS: DILOK KLAISATAPORN/ISTOCK.COM, PIXABAY.COM: PETE LINFORTH, 2541163/MALICIOUS-CODE

next

EIN BLICK IN DIE ZUKUNFT: CYBERKRIMINALITÄT

DEEPFAKES
MANIPULATION DER MASSEN

Deepfakes sind Fotos oder Videos, die mithilfe von Künstlicher Intelligenz (KI) erstellt werden. Sie zeigen zum Beispiel Personen in Situationen, die nie stattgefunden haben, und wirken täuschend echt. Mit der Weiterentwicklung der KI-Technologie wird es immer einfacher, Deepfakes zu erstellen und damit die Bevölkerung zu manipulieren. Wird es künftig überhaupt noch möglich sein, echte von unechten Bildern zu unterscheiden?

GOLDEN SHIELD
CHINESISCHE MAUER DIGITAL

Mit dem «Golden Shield» überwacht und zensuriert China den Zugang zum Internet. Laut Greg Walton vom Internationalen Zentrum für Menschenrechte und Demokratische Entwicklung wurde dadurch eine «massive, allgegenwärtige Überwachungsmaschinerie geschaffen». Andererseits zeigt Golden Shield auch, dass sich Websites, die gegen landesspezifische Gesetze verstossen, durchaus abschalten liessen – etwas, das im Westen kaum geschieht.

CLOUD COMPUTING
SCHWEIZ ALS SICHERER HAFEN

Immer mehr Daten werden in einer Datacloud und nicht mehr auf dem eigenen Server oder Computer gespeichert. Darunter befinden sich auch heikle Informationen, die umfassend geschützt sein müssen. Die Schweiz ist sowohl in wirtschaftlicher wie auch politischer Hinsicht eines der stabilsten Länder der Welt. Schon heute gibt es hierzulande rund 100 Rechenzentren, welche Daten für Dritte speichern und sichern. Wir erreichen damit die zweithöchste Rechenzentrumsdichte Europas. Und die Marktprognosen sind positiv: In den kommenden Jahren dürften in der Schweiz zahlreiche weitere Dataclouds entstehen.

QUANTENCOMPUTER
NEUSTE RECHNER-GENERATION

Noch gibt es sie nur als Prototypen, doch ihr Potenzial ist riesig: Quantencomputer könnten in Zukunft gewisse Rechenoperationen tausendfach schneller durchführen als herkömmliche Computer. Man befürchtet, dass es für sie ein leichtes sein wird, alte Datenbanken zu knacken. Denn diese sind oft mit einer für dieses Problem unwirksamen Verschlüsselungssoftware ausgestattet. Besonders gefährdet sind die Archive von staatlichen Organisationen: Sie müssen über Jahrzehnte geheim gehalten werden und sind relevant für die Staatssicherheit.

FOTOS: ELENABSL/SHUTTERSTOCK.COM, GERD ALTMANN/PIXABAY.COM, JOHN D/ISTOCK.COM