PRIVATE CLIENT LETTER

Herausgeberin: Private Client Bank AG, Zürich | T +41 44 253 73 00 | privateclientbank.ch 1. Oktober 2024 | Q4/24

KATZ UND MAUS

Eigentum wird heute in digitalen Datenbanken gespeichert, gehandelt und verarbeitet. Diese sind Ziel einer stark wachsenden Industrie von Cyberkriminellen. Der Schutz erfordert Wachsamkeit und eine professionelle Infrastruktur.

"Wie man eine Maus fängt» steht auf dem dicken Handbuch, das der oft etwas schwerfällige Kater Tom mit einem Knall zuschlägt. Mit einem wühlenden Griff schnappt er sich den im Buch eingeklemmten Mäuserich Jerry und triumphiert. Wie so oft aber gelingt es der Maus, sich aus der misslichen Situation zu befreien und die wilde Verfolgungsjagd beginnt von Neuem. Die Szene aus dem 1944 erschienenen und mit einem Oscar prämierten Zeichentrickfilm «Mouse Trouble» ist zeitlos, ebenso wie die gesamte seit über achtzig Jahren in unzähligen Varianten produzierte Cartoon-Serie «Tom und Jerry». Sie steht für ein nicht enden wollendes, meist eskalierendes Katz- und Maus-Spiel mit grossem Erfindungsreichtum und wechselnder Fortüne. Kaum glaubt einer der beiden, den Erfolg für sich gepachtet zu haben, geht es wieder in die andere Richtung. Und so sind es auch diese Comics, die kürzlich den roten Faden für die Präsentation einer der führenden Schweizer Firmen für digitale Sicherheit zur Abwehr von Cyberkriminalität bildeten. Doch trotz des humoristischen Rahmens für die Botschaft ist das Thema ernst und höchst aktuell.

Die drittgrösste Ökonomie der Welt

Schon seit längerem sind Fragen der Daten- und Cybersicherheit nicht mehr nur etwas für Informatik- und Compliance-Abteilungen von grossen Firmen. Immer häufiger werden aufsehenerregende Fälle von Erpressungen durch Hacker bekannt, wie etwa der Angriff auf die Neue Zürcher Zeitung (NZZ) im März 2023, den die Zeitung ein Jahr später öffentlich mit einem detaillierten Protokoll aufgearbeitet hat. Die NZZ ist in guter Gesellschaft: Anwaltskanzleien sind darunter, Banken, Versicherungen, Industriefirmen, Dienstleister, ja auch die britische Post oder die Stadt Dallas in den USA. Erpresserische Cyberangriffe sind an der Tagesordnung, Tendenz stark steigend. Im Fokus stehen natürlich auch vermögende Privatpersonen und Family Offices. Gemäss einer neuen Umfrage der US-Bank JP Morgan war jedes vierte befragte Family Office bereits Opfer einer Cyberattacke. Gleichzeitig hatten zwanzig Prozent der befragten Institute noch keine nennenswerten Massnahmen gegen Cyberangriffe eingeführt. Entsprechend hat die US-Grossbank ein eigenes «Global Cyber Advisory Team» eingerichtet und produziert Videos, um vermögenden Kunden Ratschläge für den Umgang mit Kriminalität im Internet zu geben.

Obwohl das Thema Datensicherheit heute überall präsent ist, unterschätzen viele Firmen und Privatpersonen die Risiken noch immer. Dabei sind inzwischen hochprofessionelle Wertschöpfungsketten am Werk, die den Vergleich mit weniger dubiosen Industrien rein betriebswirtschaftlich

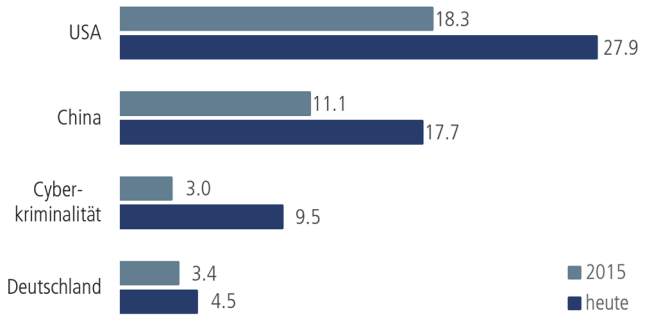
Private Client Bank AG
Alte Börse
Bleicherweg 5 – Postfach
8034 Zürich – Schweiz

T +41 44 253 73 00
F +41 44 253 73 20
info@privateclientbank.ch
privateclientbank.ch

nicht zu scheuen brauchen. So werden Daten zunächst im Netz wie mit einem Staubsauger gesammelt, ergaunert und günstig angeboten. In einem nächsten Schritt werden diese auf vielversprechende Datensätze wie potenzielle Zugänge zu Bankkonten oder Firmennetzwerken gefiltert, verarbeitet und zu höheren Preisen weiterverkauft. Die Königsdisziplin ist schliesslich die Entwicklung und Anwendung von Erpressungssoftware sowie die Verhandlung mit den Opfern, bei denen rasch auch hohe Millionenbeträge auf dem Spiel stehen.

BIP BZW. KOSTEN CYBERKIMINALITÄT IN 1'000 MRD. USD

USA, CHINA, CYBERKRIMINALITÄT



Quelle: Statista, Bloomberg, Cybersecurity Ventures, 2024.

Glaubt man der auf Cyberökonomie spezialisierten Analysefirma Cybersecurity Ventures, dann betragen die Kosten der Cyberkriminalität 2024 9'500 Milliarden US-Dollar pro Jahr. In der globalen Rangfolge der Volkswirtschaften würde die dunkle Seite der Internetökonomie hinter den USA und China auf Platz drei landen, weit vor Deutschland (siehe Grafik). Mit 15 Prozent pro Jahr sind die Wachstumsraten ausserdem enorm. Das überrascht nicht, sind doch alle digitalisierten Personen und Organisationen potenzielle Opfer bzw. «Kunden». Und in Zeiten von geopolitischen Spannungen nehmen unfreundliche staatliche und parastaatliche Aktivitäten stark zu. Für die Staaten, deren zentrale Aufgabe die innere und äussere Sicherheit ist, rückt das Thema damit nach ganz oben auf die Agenda. Das gilt bei uns nicht zuletzt auch für die Finanzmarktaufsicht, da die Sicherheit von Banken und Versicherungen für die Wirtschaft zentral ist. Deshalb treibt in der Schweiz die Finma das Thema Cybersicherheit mit grösstem Nachdruck voran.

Daten, Daten, Daten

In einem Punkt unterscheiden sich Cyberkriminelle nicht von herkömmlichen Einbrechern, Post- oder Bankräubern: Sie suchen Geld oder etwas, das zu Geld führt. Wer etwas besitzt, sollte sich also keine Illusionen machen. Anders als früher werden Vermögenswerte heute immer seltener physisch, sondern in aller Regel elektronisch aufbewahrt. Das gilt nicht nur für Geld oder Sachwerte, sondern auch und vor allem für den Nachweis über das Eigentum: Der Besitz etwa von Immobilien (Grundbuch), Wertpapieren (Aktienbuch, etc.) wird nur noch selten wirklich physisch festgehalten. Kaum auszudenken, wenn diese Nachweise aus irgendwelchen Gründen einmal gelöscht, überschrieben oder unbrauchbar gemacht würden. Eigentum liesse sich nicht mehr zuordnen und nachweisen, das Chaos wäre perfekt.

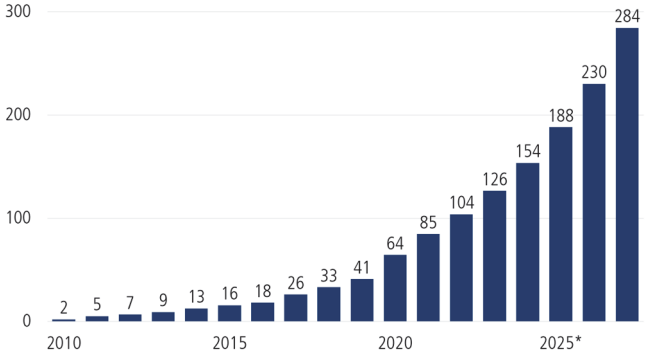
Nach dem Gesagten steht fest, dass das ewige Katz- und Maus-Spiel sich primär in die digitale Welt verlegt hat. Die Zeiten, in denen der Dorfpolizist auf der Strasse patrouillieren und für Ordnung sorgen konnte, sind vorbei. Überfälle finden heute kaum mehr mit der Pistole statt, sondern über Mobile, Tablet, PC, Firmennetzwerke, Datencenter und Internetleitungen. Die Pistole von heute ist der Totenkopf auf dem Bildschirm. Gemäss Untersuchungen der International Data Corporation (IDC) in den USA wird eine durchschnittliche, vernetzte Person im Jahr 2025 Tag und Nacht alle 18 Sekunden einen virtuellen Datenaustausch haben, und sei es nur über Positionsdaten des Mobiltelefons oder ein mit dem Netz verbundenes Fahrzeug. 2020 betrug dieser Wert pro Kopf noch 144 Sekunden, 2010 waren es 17 Minuten. Wie unsere Graphik auf der nächsten Seite zeigt, wachsen die pro Jahr generierten virtuellen Daten exponentiell. Gerechnet wird in Zettabyte: Würde man alle 2024 generierten 154 Zettabyte auf herkömmliche DVDs laden und diese übereinanderlegen, könnte man damit fast 200 Mal die Erde umrunden. Noch vor drei Jahren waren das weniger als halb so viele. Viel Stoff für Kriminelle.

Natürlich werden nicht alle diese Daten gespeichert. Sie lassen sich auch nicht alle kriminell verarbeiten, vieles ist belanglos oder für Diebstahl,

Betrug und Erpressung nutzlos. Persönliche Finanzdaten und Zugänge zu solchen Daten machen nur einen verschwindend kleinen Teil des riesigen Datenmeers aus. Auf sie aber haben es Cyberkriminelle besonders abgesehen, so dass das Schutzniveau hier auch entsprechend hoch sein muss. Das mag selbstverständlich klingen, kann aber gerade in der heutigen Zeit nicht genug betont werden. Denn allzu oft muss es gerade in Finanzdingen schnell gehen und bequem sein. Dabei gibt es trotz aller Fortschritte in der Technologie immer einen Trade-Off zwischen Sicherheit und Komfort. Und nicht zuletzt gilt: Sicherheit gibt es nicht gratis.

DIGITALE DATEN IN ZETTABYTE, PRO JAHR GENERIERT

DATENBERGE



Quelle: Statista, 2024. Die Daten stammen von der International Data Corporation (IDC), USA. Ab 2023 handelt es sich um Prognosen (*).

Wer einmal ein modernes Datencenter besuchen durfte, in dem sensitive Daten verarbeitet und gespeichert werden, dem erschliesst sich die Komplexität der Datensicherheit in der heutigen Zeit besser. Es beginnt beim physischen Schutz. So arbeitet man sich durch mehrere Schichten und Stockwerke an Sicherheitsarchitektur: Zugangskontrollen inklusive Vereinzelungsanlagen, redundante Systeme für Kühlung, für Produktion von Elektrizität bei Stromausfall, für die Verteilung des Stroms, Vorkehrungen zur Verhinderung von Wassereinbruch und Feuer, konstante Kameraüberwachung und vieles mehr. Ganz unten, mehrere Stockwerke unter dem Boden, anonym und nur für autorisierte Personen zugänglich, befindet sich der Käfig für die Speicherung und Verarbeitung der wertvollen Bankdaten – klein und unscheinbar, ein moderner Hochsicherheitstresor.

Handbuch für digitale Sicherheit

Eine Datenfestung ist aber noch keine Cyberfestung. Für ein zeitgemässes Sicherheitsdispositiv braucht es mehr: Unter anderem müssen Programme konstant auf dem neuesten Stand sein und Systemzugänge auf (mindestens) zwei verschiedenen Wegen stattfinden («Multi-Factor-Authentification»). Bei Firmen mit besonders sensiblen Daten sollten die Systeme Tag und Nacht von einer spezialisierten Sicherheitsfirma überwacht, notfalls auch unterbrochen werden können. Technologie und Prozesse müssen ständig auf Sicherheit überprüft werden, am besten durch externe Spezialisten. In unserer Bank sind wir nicht zuletzt davon überzeugt, dass der Bankenstatus und die damit verbundenen Auflagen ein dauerndes Fitnessprogramm gerade auch in Bezug auf Daten- und Prozesssicherheit sind – Vermögensverwalter sind ja nichts anderes als Unternehmen zur Verarbeitung und Aufbewahrung von Vermögensdaten.

Die grösste Schwachstelle im Bereich Datensicherheit sind aber nach wie vor wir Menschen. Wir lassen Daten liegen und sperren unsere Geräte nicht, wir geben auf sozialen Netzwerken Informationen über uns und unsere Firma preis, wir lassen uns psychologisch unter Druck setzen, weil etwas schnell gehen muss, wir klicken aus Neugierde oder Nachlässigkeit auf Links, die wir nicht antasten sollten, wir schreiben unsere Passwörter neben dem Computer auf – und vieles mehr. Als Firma sind wir deshalb überzeugt, dass der Muskel der Aufmerksamkeit in Sachen Sicherheit kontinuierlich geschult werden muss. Das gilt nicht nur für uns, sondern auch für unsere Kunden. Und auch das sei gesagt: In einem solchen Umfeld ist das Bankkundengeheimnis mit seiner strafrechtlichen Komponente alles andere als aus der Zeit gefallen.

Die Spirale der technischen Aufrüstung im ewigen Katz- und Maus-Spiel geht bereits weiter. So werden etwa Deep-Fake Videos und Stimmenimitate für falsche Zahlungsaufträge genutzt. Sollte man den Zahlungsverkehr vollständig von der Vermögensverwaltung trennen? Kein Zweifel, das Handbuch für Tom wird nie fertig werden.

—

IA, 30.09.2024

Private Client Bank AG
Alte Börse
Bleicherweg 5 – Postfach
8034 Zürich – Schweiz

T +41 44 253 73 00
F +41 44 253 73 20
info@privateclientbank.ch
privateclientbank.ch

GRUND ZUM OPTIMISMUS

"Wenn den einen Pagers um die Ohren fliegen und den andern Drohnen aufs Haupt donnern und noch andere offen mit dem Einsatz von Atomwaffen drohen, wenn in Europa eine Regierung nach der anderen zu implodieren scheint, wenn die wichtigste Notenbank der Welt ihre Leitzinsen fast panikartig senkt, dann kann beim besten Willen nicht behauptet werden, die Welt befinde sich in quasiparadiesischem Zustand. Nein, das Gegenteil scheint der Fall: schwierige, ja unlösbar erscheinende Konflikte rund um den Globus, unfähige, unredliche bis kriminelle Gestalten an entscheidender Stelle, schiefe, ins Nirwana der Knechtschaft und der gesellschaftlichen Auflösung führende Entwicklungspfade, Schuldenstände wie kaum je zuvor und eine Nonchalance sondergleichen im Umgang damit.

Vielleicht haben wir auf der realen Seite der Welt etwas übersehen. Etwas sehr Beruhigendes. Was die Welt auf Jahre hinaus zu stabilisieren in der Lage ist.

Eine solche Anhäufung von Unbill müsste sich doch irgendwie an den Entwicklungen der Finanzmärkte ablesen lassen, würde man meinen. Doch nichts von alledem. Nicht nur haben sich in diesem Jahr viele wichtige Aktienindizes ganz erfreulich entwickelt und sind die Währungsrelationen recht stabil geblieben, vielmehr - und bedeutsamer - haben sich die Risikoprämien im Kreditmarkt normalisiert und sind die Volatilitäten, das Risikomass für alle schwankenden Preise, auf historischen Tiefständen angelangt. Woher rührt solche Zuversicht, ja, vielleicht, Sorglosigkeit?

Vielleicht haben wir auf der realen Seite der Welt etwas übersehen. Etwas sehr Beruhigendes. Was die Welt auf Jahre hinaus zu stabilisieren in der Lage ist.

Ja. So ist es. Wir meinten nämlich, die USA stünden kurz vor dem Kollaps. Denn es zeichneten sich Präsidentschaftswahlen zwischen einem Unwählbaren (weil am Abgrund einer Altersdemenz stehend) und einem Unberechenbaren ab. Mit der möglichen, ja greifbar wahrscheinlichen Folge einer tiefen Verfassungskrise, ja, einer Gefährdung der Demokratie als solcher. Doch immer dann, wenn es in Amerika am dunkelsten wird, rappelt sich die Nation auf. So scheint sich auch dieses Mal das alte Dictum von Winston Churchill zu bestätigen: «Man kann sich immer darauf verlassen, dass die Amerikaner das Richtige tun, aber erst nachdem sie alles andere ausprobiert haben.» Die Wahlen sind gerettet. Es geht hier nicht um spezifische Personen. Sondern ums System. Eine Demokratie unterscheidet sich von einer Autokratie dadurch, dass die Nachfolge geordnet erfolgt. Das macht sie derart überlegen.

Damit werden die USA weiterhin führende Nation der freien Staatenwelt bleiben können, imperialistische Allüren hin oder her. Der grösste freie Kapitalmarkt der Welt wird uns erhalten bleiben, mit ihm der unaufhaltsame, weil logische Trend zur Fortsetzung der Globalisierung. Ohne die USA könnten wir die freie Marktwirtschaft, den Kapitalismus, ein einigermassen vernünftiges Wirtschaftswachstum vergessen. Europa kann's nicht alleine richten. Wir brauchen den starken Partner auf der andern Seite des Atlantiks. Die Rettung echter Wahlen und mithin den USA als Institution sind die besten Nachrichten schlechthin, an den Märkten aber noch nicht vollständig eingepreist. Es kann weitergehen, der Weltuntergang ist vorderhand wieder einmal aufgeschoben.

—

KH, 30.09.2024

Private Client Bank AG
Alte Börse
Bleicherweg 5 – Postfach
8034 Zürich – Schweiz

T +41 44 253 73 00
F +41 44 253 73 20
info@privateclientbank.ch
privateclientbank.ch