«Sicherheit ist ein Teamsport»

Er gilt als Mahner der ersten Stunde, wenn es um Risiken aus dem Cyberspace geht: Nicolas «Nick» Mayencourt. Mit seiner von ihm in den 1990er-Jahren gegründeten Firma Dreamlab kümmerte er sich schon um Cybersicherheit, als noch kaum jemand danach fragte. Im Gespräch mit uns bezeichnet er die Lage als dramatisch.

VON THOMAS BERNER

Derzeit dominieren die kriegerischen Auseinandersetzungen in der Ukraine und im Nahen Osten die Schlagzeilen. Doch nicht nur mit Panzern, Flugzeugen, Drohnen und Raketen wird aus allen Rohren gefeuert, sondern auch mit Bits und Bytes. Seit Ausbruch des Ukrainekriegs vor mehr als 20 Monaten hat sich die Lage im Cyberspace massiv verschärft. Immer mehr geraten auch Unbeteiligte – Private, Firmen, öffentliche Verwaltungen – zwischen die Fronten des Cyberkriegs, weiss Nicolas Mayencourt. Wir sprachen mit ihm im Vorfeld der Swiss Cyber Security Days, die am 20./21. Februar 2024 stattfinden.

Herr Mayencourt, wir führen dieses Interview per Videocall. Müssen wir uns um unsere Cybersicherheit hier ernsthafte Sorgen machen?

NICOLAS MAYENCOURT: Das kommt etwas darauf an. Zum einen werden die Kanäle zum Endpunkt hin verschlüsselt – sichtbar an der Bezeichnung «https» im Browser. Das ist schon mal gut für die Sicherheit. Aber zum anderen führen wir Codes eines Cloud-Anbieters in unseren Browsern aus. Dabei könnte es sich auch um bösartige Codes handeln, die durch irgendwelche Wege – kriminelle oder kompromittierte Mitarbeitende des Dienstleisters oder durch Dritte – eingebracht worden sind. Das kann Ransomware sein oder Spionagesoftware. Wir haben dabei keine Chance, dies zu verifizieren; wir müssen hier einfach dem Dienstleister vertrauen – in unserem Falle Microsoft. Es gibt aber noch ein weiteres Problem.

Welches?

Den Datenschutz. Da besteht zwischen den USA, dem Heimatland von Microsoft, und Europa ein gravierender Unterschied. In den USA muss jede kommerzielle Firma den Behörden Zugang zu ihren Daten gewähren, unabhängig davon, in welchen Ländern sie ihre Server betreibt. Die Daten gehören somit auch dem Staat. Davon betroffen sind also auch unsere Daten, die wir Microsoft anvertrauen. Denn diese sind gemäss amerikanischer Auslegung Eigentum des Providers. Dies im Gegensatz zur europäischen Rechtslage, wo die Daten der Person gehören, die sie generiert, auch wenn sie bei einem Host, einem E-Mail-Provider oder gar einer staatlichen Institution gelagert sind. Es besteht also zwischen der europäischen und der amerikanischen Denkweise eine Inkompatibilität.

Wie viel unsicherer ist die Cyberwelt nach Ausbruch des Ukrainekriegs und jetzt im Zuge der Nahostkrise geworden?

Der Ausbruch des Ukrainekriegs bedeutete einen Dammbruch. Zunächst kam Corona. Es machte peng, und die Fälle von Ransomware schnellten durch die Decke. Cyberkriminelle begannen massiv, Private und Unternehmen auszurauben. In einer

FOTO: DEPOSITPHOTOS.COM


CYBER WARFARE

ersten Welle ging es ihnen nur darum, Daten zu verschlüsseln und gegen Lösegeld wieder zu entschlüsseln. Dann merkten sie schnell, dass sie mit ihren Aktivitäten auf wertvolle Insights – Buchhaltung, Login-Daten, Forschungsergebnisse, Produktionsdaten und andere Geschäftsgeheimnisse – gestossen sind. Ein wahrer Schatz, an dem Mitbewerber oder sogar staatliche Geheimdienste gewiss ein grosses Interesse haben und für den sie viel Geld zahlen dürften … Das hat sich in den letzten zwei bis drei Jahren massiv hochgeschaukelt. Stellen Sie sich vor: So viele Daten, die nun von Wettbewerbern und Geheimdiensten überall auf der Welt «studiert» werden! Dies führt zu einer gewaltigen systemischen Instabilität. Dem legte der Ukrainekonflikt gleich noch eine Schippe drauf: Da reden wir nicht von einer Explosion im Quadrat, sondern von Kubik!

Sie dramatisieren!
Nein. Es gab da die weltgrösste Ransomware-Gruppe namens Conti, eine ukrainisch-russische Organisation von Kriminellen. Mit Ausbruch des Ukrainekriegs kam es dort zur Implosion: Während die russische Fraktion von der Richtigkeit der russischen Sache überzeugt war, trug dies die ukrainische Seite nicht mehr mit. Sie veröffentlichte daraufhin Interna, wie die Organisation arbeitete. So wurde offensichtlich, wie die «Kooperation» zwischen Staat und Cyberkriminellen in Russland schon lange gang und gäbe war – nett ausgedrückt: eine «Public Private Partnership» mit negativen Vorzeichen. Das heisst: Die Regierung toleriert, ja schützt und unterstützt kriminelle Organisationen. Als «Gegenleistung» wird verlangt: keine Angriffe auf russische Ziele, ordentliche Bezahlung von Steuern und – wenn gefordert – Bereitschaft, dem Staat Unterstützung zu leisten. Es handelt sich also um eine Vermengung von Hardcore-Hackern und russischen Regierungskreisen. Und das wird systematisch genutzt. So störte etwa eine russische Splittergruppe das GPS-System. Davon betroffen war übrigens auch die Schweiz. Zur Potenzierung des Risikos trägt auch bei, dass 300 000 Hacker wie z.B. Anonymous ihren eigenen «Krieg» für die Ukraine gegen Russland führen. Niemand, kein Staat, trägt hier die Verantwortung dafür. Was passiert also, wenn es wegen eines solchen Hackerangriffs mal zivile Tote gibt? Wer wird dann zur Rechenschaft gezogen?

Das ist in der Tat beunruhigend. Indes erhält man bei vielen Unternehmen immer noch den Eindruck: Cyberrisiken haben andere, aber nicht wir. Worauf führen Sie diesen Zustand, sich in falscher Sicherheit zu wiegen, zurück?
Da ziehe ich gerne den Vergleich zum Klimawandel: Es ist einfach zu sagen, es gebe ihn nicht, wenn man draussen einen schönen Herbsttag geniesst. Dann sieht man vielleicht in einer Dokumentation die schmelzenden Gletscher und ist berührt. Aber fünf Minuten später geht man wieder nach draussen in den schönen Herbsttag – und alles ist wieder vergessen. Mit anderen Worten: Es schmerzt zu wenig! Oder ein anderes Beispiel: 2022 verbuchte die Welt mehr als 5 Billionen (!) Franken an Cyberschäden. Das ist 48 Mal mehr als alle globalen Naturkatastrophen zusammen. Das entspricht dem Volumen der weltweit drittgrössten Volkswirtschaft! Das ist ein finanzieller Schmerz, unter dem sämtliche Versicherer ächzen und sagen: Diese Schäden lassen sich nicht mehr versichern. Die Wucht an krimineller Energie ist gewaltig: Nur schon dieses Jahr wurden Websites des Bundes mit einer DDoS-Attacke gehackt, die SBB konnten einen Tag lang keine Tickets verkaufen, Xplain leakte Dokumente aus unserem Verteidigungsministerium. Das ist erschütternd und müsste bei allen von uns Gänsehaut erzeugen. Aber eben: Wir kriegen jeden Monat unseren Lohn, haben ein Dach über dem Kopf, haben es warm und genügend zu essen – ein schönes Leben also.

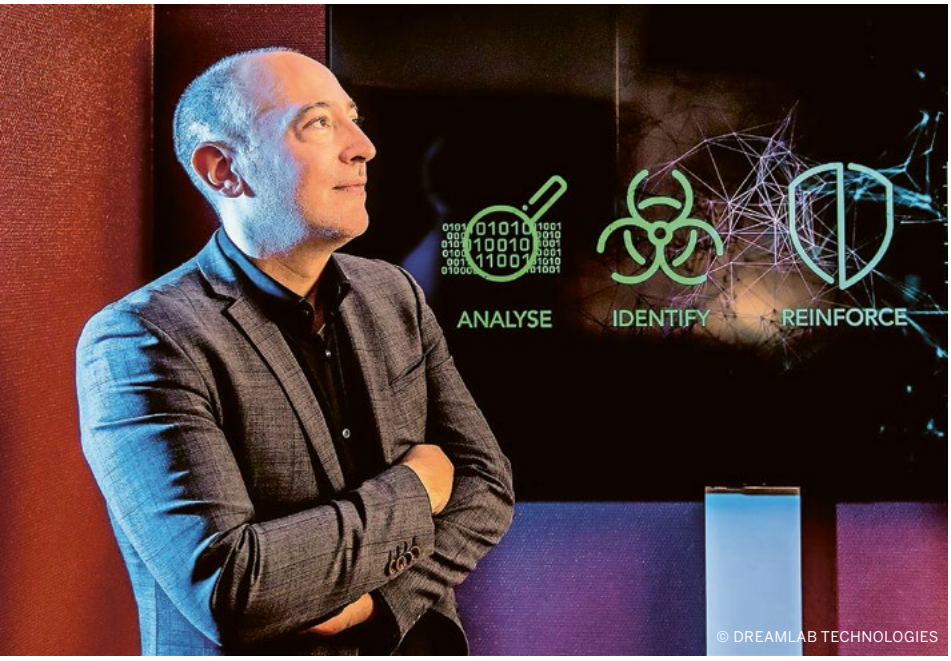
Das heisst, wir reagieren erst, wenn es physisch schmerzt – frei nach dem Motto: «Aus Schaden wird man klug»?
Ich glaube schon, ja. Unser Körper ist für die Natur gemacht, nicht für den Cyberspace. Dort ist alles kognitiv, alles entzieht sich der sinnlichen Erlebbarkeit. Ein Cyberangriff tut eben nicht physisch weh, wir «spüren» nicht, wenn es einem Gerät schlecht geht. Aber gerade der Cyberspace und die Geräte durchdringen inzwischen jede Lebenslage von uns. Kurz, wir leben mit einem mehrere Zehntausend Jahre alten Körper in einem Regulativ ähnlich dem Römischen Reich und tragen quasi gottgleiche Technologie in unseren Händen. Das ist eine riesige Dissonanz. Das führt dazu, dass wir mit einem Lächeln den schönen Herbsttag geniessen, und gleichzeitig finden Klimawandel und Cybergeddon statt. Das ist das, was mich traurig stimmt. Wenn man sich aber mal die Zeit nimmt, kognitiv in den Cyberraum hineinzutauchen, wird man zur Schlussfolgerung kommen müssen, dass wir alles besser machen müssen.

Das Motto der Swiss Cyber Security Days vom 20. und 21. Februar 2024 lautet: Shaping Cyber Resilience. Das impliziert: Eine hundertprozentige Sicherheit gibt es nicht, deshalb muss man resilienter werden und auch mal einen Vorfall aushalten können. Wie kann man also lernen, mit dem Restrisiko umzugehen?
Sie sehen das völlig korrekt: Eine hundertprozentige Sicherheit gibt es nicht und wird es nie geben. Doch 95 Prozent der Sicherheit sind erreichbar und gar nicht teuer: Multifaktorauthentifizierung, VPN, Angriffsflächenreduzierung, Datenverschlüsselung sowie unlöschbare Back-ups. Mit diesen Massnahmen ist man vor Billig-

Zur Person

Nicolas Mayencourt ist Gründer und Geschäftsführer des IT-Sicherheitsunternehmens Dreamlab Technologies, das seit über 20 Jahren Sicherheitskonzepte und -lösungen erarbeitet. Zudem ist er Programmdirektor der Swiss Cyber Security Days, die vom 20. bis 21. Februar 2024 in Bern stattfinden.

> *www.scsd.ch*



Nicolas Mayencourt: «95 Prozent der Sicherheit sind erreichbar und gar nicht teuer.»

Ransomware geschützt und das Gros der Risiken hat man eliminiert. Ich nenne das nicht einmal Cyber-Security, sondern Cyberhygiene. Wenn wir alle dies umsetzen, müssten wir nur noch über die restlichen fünf Prozent reden. Diese sind unendlich komplex, teuer und ein gigantisches Problem. Deshalb wird es eine hundertprozentige Sicherheit auch nie geben können, denn das wäre wirtschaftlich nicht stemmbar. Genau dort setzt nun die Resilienz an. Für KMU bedeutet Resilienz: Auf die restlichen fünf Prozent vorbereitet sein, z.B. wissen, wie man das Back-up oder die Firmenwebsite restauriert, wissen, wen man kontaktieren muss – mit physisch greifbaren Telefonnummern und Notfalladressen. Es geht also um Vorsorge, um Notfallpläne, um ein funktionierendes Business Continuity Management. Und das muss man auch gelegentlich üben, damit man schnell wieder am Start sein kann. So lässt sich ein Millionenschaden oder gar ein Konkurs abwenden.

«2022 verbuchte die Welt mehr als 5 Billionen (!) Franken an Cyberschäden.»

Im Prinzip dasselbe, das man unternimmt, um gegen einen Elementarschaden wie z.B. Feuer gewappnet zu sein?

Das ist eine gute Analogie. Denn so wie man Brandschutzkonzepte mit Brandmauern – physischen Firewalls – ausarbeitet, Brandschutzvorschriften einhält, Evakuierungspläne hat, so verhält es sich auch bei Cyberrisiken. Das ist mal die «KMU-Skala». Doch Cyber verbindet alle mit allen. Deshalb müssen wir auf einer Welt-Skala denken. Denn kein Staat ist bezüglich Cybersicherheit autark. Cybersicherheit ist ein Teamsport; Resilienz kann nur funktionieren, wenn man sich gegenseitig unterstützt. Es gilt also, gemeinsam Rezepte zu finden, um die Verteidigungsdispositive im Cyberspace zu härten. Man muss vor allem Wege finden für eine bessere internationale Kooperation, etwa bei Rechtshilfegesuchen, und gescheite Plattformen für Datenaustausch und Joint Forces schaffen.

Kann KI bei der Cyberabwehr helfen?

Künstliche Intelligenz hat gewiss einen Nutzen: Machine-Learning-Algorithmen helfen etwa bei der Erkennung von Sicherheitsbedrohungen, indem sie automatisiert Muster und Anomalien identifizieren. KI ermöglicht auch eine effiziente Überwachung der Netzwerkaktivität, indem sie die Analyse des normalen Netzwerkverkehrs als Grundlage nutzt. KI ist ein Schritt in der Evolution der Sicherheit, keine Revolution. Sie spielt eine Rolle bei der Verbesserung von Sicherheitspraktiken, sollte aber die Beteiligung und Entscheidungsfindung von Menschen nicht ersetzen. Es gibt auch ein Bedrohungspotenzial, Cyberangriffe mithilfe von KI und maschinellem Lernen sind schon heute eine Gefahr. Amateur-Hacker ohne Programmierkenntnisse können bspw. mit Chat GPT Sicherheitslücken in Software finden oder Ransomware schreiben. Oder Chatbots können E-Mails schreiben, die genauso klingen wie eine Anweisung eines Vorgesetzen. Cyberkriminelle brauchen kaum mehr Programmierfähigkeiten, sondern können sich Schadcode von Chatbots schreiben lassen. Weil Programme dabei auf bestehenden Code zurückgreifen, entstehen zwar nicht unbedingt qualitativ neue Angriffe. Aber das Volumen und die Kadenz bekannter Attacken nimmt zu.

Was steht an den Cyber Security Days im Zentrum?

An den Cyber Security Days reden wir über die wichtigsten Megatrends, also über den Impact von KI, Möglichkeiten von Quantencomputern für die Kryptografie und über neue Risiken, auch im Zusammenhang mit Desinformation via Fake News. Dafür wählen wir drei Arten von Vermittlung: Auf der Main Stage befassen wir uns mit dem erwähnten gesellschaftlichen Dialog. Diese Themen richten sich denn auch an ein nicht technologieaffines Publikum. Dann gibt es eine technologische Main Stage, wo es um technische Schutzmassnahmen und Prävention geht. So zeigen wir, dass Post Quantum Cryptography auch mit herkömmlichen Computern möglich ist. Wir werden auch einen AI Safety Prize schaffen: Ausgezeichnet werden Lösungen, die helfen, die Sicherheit von KI zu verbessern. Und eine dritte Ebene wendet sich explizit an KMU: Was können sie mit wenig Budget für die Cybersicherheit erreichen? Dazu liefern wir zusammen mit Anbietern von A bis Z konkrete und handfeste Antworten. Abgerundet wird dies alles durch Workshops, die sich nicht nur an KMU wenden, sondern auch an Gemeinden und Städte. Das Ziel ist, zu zeigen, wie sich jene 95 Prozent an Sicherheit erreichen lassen, die für den Schutz vor den meisten Ransomware-Angriffen bereits ausreichend sind.