« Es ist Zeit für ein radikales Umdenken »

Cyberkriminelle beuten die Angst vor dem Coronavirus aus. Und die Angriffsfläche reicht bis ins Homeoffice. Nicolas Mayencourt, CEO und Gründer von Dreamlab Technologies, spricht darüber, wie die Coronakrise unseren Umgang mit IT-Sicherheit und Datenschutz verändert, wo die grössten Gefahren lauern und was dagegen zu tun ist. Interview: Joël Orizet

« In den letzten Jahren sind wir mehrmals knapp an einer digitalen Epidemie vorbeigeschrammt. »

Nicolas Mayencourt, CEO und Gründer, Dreamlab Technologies

Wie schätzen Sie die aktuelle Bedrohungslage der IT-Sicherheit ein?
Nicolas Mayencourt: Die globale Stabilität ist durch zwei grosse Risikocluster bedroht. Erstens von Gefahren für die Gesundheit wie der Klimawandel und Viren. Wir erleben derzeit eindrücklich die Grenzen der Stabilität und Resilienz unseres Systems. Die Pandemie zeigt die Schwächen auf – beispielsweise internationale Lieferketten und Interdependenzen. Sie zeigt aber zugleich auch, wie diszipliniert und solidarisch wir handeln können. Der zweite Risikobereich ist der Cyberraum. Das Digitale durchdringt unser ganzes Leben. Ohne eine funktionierende Technologie und Cyber-Infrastruktur gibt es kein Homeoffice, keine Geschäftstätigkeit, keine Transaktionen mehr. Während im Bereich der Gesundheitsrisiken Hygienemassnahmen endlich die angemessene Bedeutung zukommt, sind entsprechende Sicherheitsvorkehrungen im Cyberraum bislang leider noch nicht überall vorhanden.

Wo sehen Sie die grössten Gefahren?
In den letzten Jahren sind wir mehrmals knapp an einer digitalen Epidemie vorbeigeschrammt. Etwa mit den Cyberangriffen, die im Jahr 2015 grosse Teile der Elektrizitätsversorgung in der Ukraine lahmlegten, einen Blackout verursachten und, weil solche Angriffe schwer einzugrenzen sind, in Folge auf die gesamte Welt zielten. Ein Erpressungstrojaner befiel 2017 über 200 000 Computersysteme in 150 Ländern, verursachte einen Schaden von mehreren Milliarden Dollar, hat beinahe die Lieferkette lahmgelegt und kostete Menschenleben. Das Schema war bei all diesen Angriffen dasselbe – wie immer: Es wurde eine kleine Sicherheitslücke im Betriebssystem ausgenutzt. Dadurch konnte die gesamte Architektur zerstört werden.

Aufgrund der Coronavirus-Pandemie boomt das Homeoffice. Wie verändern sich dadurch die IT-Sicherheitsrisiken?
Die Angriffsfläche hat sich in Summe vergrössert. Dadurch, dass nun viele von zuhause aus arbeiten, zählen auch die Home-Infrastrukturen zur Angriffsfläche von Unternehmen. Weil die Umstellung schnell gehen musste, war vielleicht nicht alles optimal vorbereitet, konfiguriert und verteidigt. Manche haben Software oder Produkte eingeführt, ohne sie genügend zu prüfen – weil sie die Arbeit von zuhause aus ermöglichen oder vereinfachen. Etwa ein Videokonferenztool mit bekannten Sicherheitsproblemen. Viele nutzen es trotzdem, da es bequem anzuwenden ist. Das schafft neue, teilweise immense Risiken. Die Bedrohungslage ist technisch die gleiche geblieben, aber die Angriffsfläche ist grösser und damit auch das Risiko, angegriffen zu werden.

Wie sieht es mit Cyberkriminalität aus?
Wir stellen eine Vervielfachung der Trickbetrügereien, Phishing- und anderen Angriffen fest. Durch die aktuelle Situation sind wir neugierig und schneller dazu zu verleitet, etwas anzuklicken, das neue Daten oder Besserung verspricht. Es gibt mehr Angreifer und mehr Angriffsaktivitäten bei zeitgleich höherer Bereitschaft, Mails zu öffnen, PDFs doppelzuklicken oder den neuen VPN- beziehungsweise Videochat-Client zu installieren. Dazu kommen Corona-Apps, die grundsätzlich legitim sind, jedoch vor ihrem Start einen Trojaner installieren. Die Kriminellen sind nicht nur erschreckend skrupellos – sie sind leider auch schnell und einfallsreich. In der aktuellen Situation sind wir stark vom Funktionieren der Technik abhängig – entsprechend gravierend wäre und ist ein erfolgreicher Angriff.

Wie verwundbar die Schweiz ist, zeigte auch Ihre Analyse der Angriffsfläche von Schweizer Spitälern: Sie fanden hunderte offene Zugänge und Schwachstellen. Hat sich die Situation inzwischen verbessert oder sind die Spitäler während der Coronakrise noch anfälliger für Cyberangriffe als zuvor?
Wir analysieren mit unserem Cyberradarsystem laufend den Zustand der Infrastrukturen in der Schweiz. Die Spitäler haben wir aus aktuellen Gründen priorisiert – ähnliche Feststellungen gibt es aber auch in anderen Bereichen. Der Prozess ist im Gang, wir sind mit den betroffenen in Kontakt und klären gemeinsam mit ihnen, wie sie die Sicherheit verbessern können. Wenn die entsprechenden Massnahmen umgesetzt werden, ist die IT der Spitäler durch unsere Studie sicherer geworden. Bei der Medizinal-IT braucht es allerdings auch strukturelle Veränderungen.

Inwiefern?
Die Konfigurationen der Spezialgeräte dürfen zum Teil nicht geändert werden, da sonst die Garantie und die Zu-

i ZUR PERSON

Nicolas Mayencourt ist Cybersicherheitsexperte mit 25 Jahren Erfahrung in der Sicherung von IT-Infrastrukturen. Er ist Gründer und globaler CEO des Cybersecurity-Unternehmens Dreamlab Technologies. Als Mitautor von OSSTMM definierte Mayencourt in den frühen 2000er-Jahren globale Cybersicherheitsstandards. Er ist unter anderem Mitglied des World Wide Web Consortium (W3C) und der schweizerischen Plattform für Cybersicherheit SCSD. In den letzten zwei Jahrzehnten unterstützte Mayencourt Unternehmen sowie Regierungsorganisationen in den Bereichen Audit, Aufbau von Cyber Defence Centers, Cybersicherheitsberatung und Politikgestaltung.
Quelle: Dreamlab Technologies

Das Interview finden Sie auch online
www.netzwoche.ch

« Digitalisierung bedeutet, dass wir die Gesellschaft neu bauen, neu gestalten – und Verantwortung dafür übernehmen, dass sie sicher ist und bleibt. »

Nicolas Mayencourt, CEO und Gründer, Dreamlab Technologies

lassung verfällt. Das verhindert das Installieren von Sicherheitspatches. Die entsprechenden Regulatorien müssen also dringend angepasst werden. Solange es bekannte kritische Lücken im Cyberspace gibt, ist auch eine erhöhte Gefahr da, dass diese für einen Angriff ausgenutzt werden. Und wie bereits gesagt, wäre ein Angriff in der jetzigen Situation besonders verheerend.

Was ist zu tun, um kritische Infrastrukturen hierzulande besser zu schützen?

Wir können nicht so weitermachen wie bisher. Die letzten zehn Jahre haben gezeigt, dass wir so nicht vorwärtskommen und stets neue Risiken schaffen. Es braucht ein radikales Umdenken, damit wir bereit sind für die Industrie 4.0, die komplett im Cyberraum stattfindet. Hier können keine technischen Verwundbarkeiten und Schwächen mehr toleriert werden – das Funktionieren der Technologie ist zu wichtig. Ähnlich wie im Strassenverkehr braucht es Fahrzeugzulassungen, Führerausweise und Verkehrskontrollen. Es gibt heute kaum mehr einen Betrieb, dessen Geschäft nicht auf Technologie basiert. Das Obligationenrecht schreibt vor, dass Geschäfte mit der nötigen Sorgfalt durchgeführt werden müssen. Hier sollten wir ansetzen: Verwaltungsrätinnen und Geschäftsleiter müssen verstehen, wie der Cyberraum gesichert wird und verantwortungsvoll damit umgehen.

Contact-Tracing-Apps stehen als Mittel zur Eindämmung der Pandemie zur Diskussion. Was halten Sie davon?

Ich bin kein Virologe, aber es leuchtet mir ein, dass eine solche App im Kampf gegen die Pandemie sehr nützlich ist. Ihr Einsatz ist aber auch mit einem hohen Risiko verbunden. Wenn beispielsweise bei allen Geräten die Bluetooth-Schnittstelle geöffnet wird – ein durchaus mögliches Szenario –, dann wächst die Angriffsfläche exponentiell. Denn natürlich können damit nicht nur die Daten dieser App übermittelt werden. Eine solche App sollte also gut geprüft werden, insbesondere ist auch Datensparsamkeit ein Thema – und wir sollten uns Gedanken über ein Exit-Szenario machen.

Was macht die Coronakrise mit unserem Umgang mit Datenschutz und Datensicherheit?

Im Moment scheint es von übergeordnetem Interesse zu sein, schützenswerte Daten preiszugeben. Bis vor Kurzem wären wir dazu nicht bereit gewesen. Es lohnt sich immer, genau hinzuschauen: Was ist zwingend nötig, wie bringen wir das später wieder weg? Klar, im Moment kämpfen wir vereint gegen einen gemeinsamen Feind. Aber wenn dieser Feind besiegt ist, möchten wir wahrscheinlich gerne unsere Privatsphäre zurück. Deshalb sollten wir auch jetzt schon Ausstiegsmöglichkeiten mit einbauen.

Viele Nutzer nehmen die Gefahren im Web zu wenig ernst. Wir seien zu naiv, sagten Sie anlässlich der letzten Ausgabe der Swiss Cyber Security Days. Was braucht es, um das zu ändern?

Wir haben die letzten 20 Jahre nicht aufgepasst. Jetzt realisieren wir die Gefahr, in die wir dadurch gelangten, dass wir unsere Daten freiwillig hergegeben haben, zum Beispiel die Meinungsbeeinflussungen im US-amerikanischen Wahlkampf mittels Facebook. Es ist Zeit für ein radikales Umdenken. Wir dürfen nicht mehr akzeptieren, dass sich Lücken in Software befinden, dass unsere Privatsphäre von Produkten unterlaufen wird. Cyberangriffe sind keine höhere Gewalt. Sie sind die Konsequenz des Einsatzes unausgereifter Produkte. Wir müssen einen verantwortungsvollen Umgang damit lernen. Und Verantwortung einfordern. Digitalisierung bedeutet nicht einfach das Nutzen von Produkten, die einem die Arbeit erleichtern, und nachträgliches Absichern. Es bedeutet, dass wir die Gesellschaft neu bauen, neu gestalten – und Verantwortung dafür übernehmen, dass sie sicher ist und bleibt.

i DIGITAL ECONOMIC FORUM

Am 12. Mai 2020 findet das erste DEF@home um 11.55 Uhr statt, das aktuelle Trends und Fragestellungen beleuchtet. Experten diskutieren über die Zeit nach Corona und wie wir die Zukunft gestalten können.

- Wie geht es mit der Digitalisierung nach Corona weiter?
- Welche Gestaltungsmöglichkeiten, Chancen und Risiken bietet die neue Situation?

Das nächste ganztägige Digital Economic Forum mit Richard David Precht findet am 15. April 2021 statt.