Cyberkriminalität und Cybersicherheit in der Zeit nach COVID-19

Juli 29, 2020
by Yotam Gutman

Das erste Halbjahr 2020 liegt hinter uns. Sicherlich hat niemand bei seinen Prognosen zu den Cybersicherheitstrends damit gerechnet, dass die ganze Welt durch ein neues Virus in so stürmische Zeiten gerät. Ganze Länder gingen in den Lockdown, der Luftverkehr kam zum Erliegen und auch die größten Unternehmen waren gezwungen, alle ihre Mitarbeiter ins Homeoffice zu schicken.

Angesichts dieser äußerst angespannten Lage ist es schwierig, Prognosen für die zweite Jahreshälfte zu treffen. Dennoch haben wir in den vergangenen sechs Monaten viel gelernt. Versuchen wir also, ein paar zuverlässige Einschätzungen abzugeben.

Allein zu Haus oder in Begleitung von Cyberkriminellen?

Beginnen wir mit den Benutzern (oder Opfern). COVID-19 hat Millionen von Angestellten nach Hause geschickt – einige dauerhaft (weil sie entlassen wurden) und andere ins Homeoffice. Dieser schlagartige Wandel scheint sich teilweise zu manifestieren. Einige der weltweit größten Unternehmen (Twitter, Facebook, Shopify, Zillow) haben bereits erklärt, dass sie das Homeoffice für eine praktikable Arbeitsoption für alle Mitarbeiter halten, die gern weiterhin so arbeiten wollen.

Selbst auf traditionelleren Märkten finden Veränderungen statt. Einer der größten Arbeitgeber Japans, Fujitsu Ltd., wird seine Bürofläche im Laufe der nächsten drei Jahre um 50 Prozent verkleinern und ermutigt 80.000 Büroangestellte, hauptsächlich von zu Hause zu arbeiten. Derzeit arbeiten 42 % der US-amerikanischen Angestellten im Homeoffice. Einige Umfragen legen nahe, dass Unternehmen selbst nach Abflauen der Pandemie, es einigen (oder allen) Mitarbeitern gestatten werden, weiterhin außerhalb des Büros zu arbeiten.

Angesichts der Millionen von Menschen, die nun im Homeoffice arbeiten, eröffnet sich böswilligen Akteuren eine enorme Angriffsfläche. Es ist nicht einfach, für all diese Mitarbeiter, die außerhalb der (relativ) sicheren Peripherie ihrer Büros und des lokalen Intranets arbeiten, das gleiche Sicherheitsniveau zu gewährleisten. Außerdem lässt bei den Mitarbeitern im Laufe der Zeit die Aufmerksamkeit nach, und es gibt zahlreiche IT-„Verlockungen“ (vielleicht dürfen die Kinder mit dem Arbeitslaptop im Internet surfen), wodurch die Anfälligkeit für Cyberkriminalität weiter zunimmt.

> *Prognose:* Das Arbeiten im Homeoffice wird ein Sicherheitsproblem für Unternehmen bleiben, sofern sie nicht in die Erweiterung und Pflege der Sicherheitsmaßnahmen für Mitarbeiter unabhängig von deren Standort investieren.

Cyberkriminelle Ansatzpunkte nach COVID-19

Cyberkriminalität hat während der COVID-19-Pandemie einen Boom erlebt. Laut dem Internet Crime Complain Center (IC3) des FBI ist die Zahl der Beschwerden über Cyberkriminalität um 300 % gestiegen.

Der Datenverkehr zu Hacking-bezogenen Websites ist angewachsen. Auch Suchen nach Informationen und Tutorials zum Thema Hacken haben in der Zeit von März bis Mai sprunghaft zugenommen. Das deutet darauf hin, dass viele so genannte „n00bs“ (Noobs, also Neulinge in der Hacker-Welt) dabei sind, sich in diesen Bereich einzuarbeiten. Viele cyberkriminelle Aktivitäten der letzten Monate standen im Zusammenhang mit dem Virus. Die Telco Security Alliance meldete allein im Monat März eine Zunahme von 2.000 % bei den Cyberbedrohungen mit COVID-19-Bezug.

Die Zahl cyberkrimineller Aktivitäten nimmt insgesamt zu, doch bestimmte Segmente sind erfolgreicher als andere. So hat zum Beispiel die Nachfrage nach gestohlenen Kreditkarten während der Pandemie nachgelassen. „Althergebrachte“ Betrugsmaschen (Werbung für gefälschte oder ungeeignete Medikamente und medizinische Ausstattung, dubiose Investitionsgeschäfte und vieles mehr) sind hingegen auf dem Vormarsch. Im Unternehmensbereich scheinen die Cyberkriminellen noch dreister geworden zu sein. Sie wenden hier sehr viel aggressivere Techniken an und zielen eher auf das schnelle Geld als auf langfristige Profite ab.

> *Prognose:* Cyberkriminalität wird zunehmen. Die Angreifer werden mit aggressiver Malware und individualisierter Ransomware verstärkt Unternehmen und Organisationen ins Visier nehmen, um sie zu bestehlen und lahmzulegen. Für schnelle Gewinne werden die Kriminellen in größerem Umfang Taktiken wie Erpressungen anwenden, bei denen die Opfer ein Lösegeld zahlen müssen, um die Veröffentlichung oder Versteigerung gestohlener Informationen zu verhindern.

Polizeiliche Cyberüberwachung: Sind die Guten bald besser?

Behörden wissen über diese Situation Bescheid und arbeiten daran, die Bedrohungen zu entschärfen. Ausgangspunkt dafür ist die verstärkte Kooperation zwischen den Ländern, etwa im Rahmen der Partnership Against Cybercrime (Partnerschaft gegen Cyberkriminalität) des Weltwirtschaftsforums. Die im April 2020 ins Leben gerufene Initiative hat die Aufgabe, die öffentlich-private Zusammenarbeit zu erweitern und globale Cyberkriminalität zu bekämpfen. Auch die Kooperation zwischen nationalen Strafverfolgungsbehörden soll sich verstärken und zeigt bereits erste hervorragende Ergebnisse. Wir sind zum Beispiel Zeugen der Ausschaltung von EncroChat (einem verschlüsselten Telefonnetz, das bei Kriminellen sehr beliebt war) durch die französische und niederländische Polizei.

Die Strafverfolgungsbehörden machen zudem Fortschritte bei ihren Bemühungen, die Meldung von Cyberkriminalität zu vereinfachen. Das britische National Cyber Security Center hat beispielsweise eine spezielle E-Mail-Adresse für die Meldung von Online-Betrug eingerichtet. In weniger als zwei Monaten sind bereits eine Million (!) Beschwerden eingegangen.

Der US-Bundesstaat Michigan hat ein ähnliches Angebot, und zwar eine Telefonnummer, unter der Anrufer rund um die Uhr kostenlos Unterstützung und Beratung in Bezug auf Cyberkriminalität erhalten. Großbritannien greift außerdem auf aktivere Maßnahmen zurück, etwa die Lancierung einer bezahlten Online-Werbekampagne, die junge Menschen ansprechen soll, die nach Cyberkriminalitäts-Services suchen, und ihnen stattdessen seriöse Alternativen anbietet.

> *Prognose:* In der polizeilichen Cyberüberwachung durch internationale und nationale Behörden wird sich die Zusammenarbeit verbessern und die Überwachung wird effizienter werden, sodass mehr Cyberkriminelle ihrer gerechten Strafe zugeführt werden können.

Hacktivismus: Ein gefährliches Spiel

Auch wenn keine finanzielle Motivation dahintersteht, sind Cyberaktivisten in letzter Zeit stärker hervorgetreten. Die jüngsten sozialen Unruhen in den USA haben eine Welle von Hacktivismus-Aktivitäten ausgelöst, darunter DDoS-Angriffe auf Stadtverwaltungen und Polizeidienststellen. In diesem Jahr haben wir Datenlecks von Millionen von Polizei- und FBI-Datensätzen sowie aggressive Social-Media-Angriffe auf die US-Regierung, Präsident Trump und sogar die beliebte Social-Media-App TikTok erlebt.

Diese Aktivitäten stellen zwar keine direkte Gefährdung für Gesellschaften und Einzelpersonen dar, können sich jedoch gegen einzelne Personen oder Organisationen richten, die als Gegner der Grundsätze der Hacker-Gemeinschaft wahrgenommen werden.

> *Prognose:* Hacktivismusaktionen stehen in engem Zusammenhang mit dem Zeitgeschehen und sozialen Unruhen. Die weitere Entwicklung hängt stark von der Situation in den USA und den Ereignissen im Vorfeld der US-Wahlen 2020 ab. Wenn sich eine Nation im Krieg mit sich selbst befindet, führt dies unweigerlich zu einer Zunahme von Hacktivismusaktivitäten.

Fazit

In den letzten sechs Monaten war alles anders. Es ist noch zu früh, um die langfristigen Auswirkungen der COVID-19-Pandemie abschätzen zu können. Ziemlich sicher lässt sich jedoch sagen, dass diese Zeit für den größten Wandel in der Arbeitswelt seit Erfindung des modernen Büros sorgt. Das führt auch dazu, dass Unternehmen, Organisationen und Einzelpersonen deutlich anfälliger für böswillige Cyberaktivitäten werden.

Doch es gibt nicht nur schlechte Nachrichten: Die Strafverfolgungsbehörden haben das Problem in seinem vollen Umfang erkannt und verstärken ihre Zusammenarbeit. Den Unternehmen muss klar werden, dass sie die Situation beeinflussen können. Verringern Sie Ihr Risiko, indem Sie eine leistungsfähige verhaltensbasierte KI-Lösung nutzen, die Schäden verhindert, erkennt und behebt, die bekannte und unbekannte Bedrohungen verursachen. Zwingen Sie Cyberkriminelle, sich woanders nach dem schnellen Geld umzusehen. Wenn Sie wissen möchten, wie SentinelOne Sie dabei unterstützen kann, Ihr Unternehmen – die Mitarbeiter im Büro und im Homeoffice – zu schützen, kontaktieren Sie uns noch heute oder fordern Sie eine kostenlose Demonstration an.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Verhaltensbasierte KI: Der uneingeschränkte Schutzansatz für Unternehmen
- Die 10 besten Methoden zum Schutz des Active Directory