Darum verhindert Cybersecurity unwissentliche Mittäterschaft

Cyberkriminalität kommt ohne Pistolen aus. Daten jeder Art können ihr Treibstoff geben. Wer die organisierte Kriminalität im Internet nicht füttern und indirekt zum Mittäter werden will, sollte sich schützen. Sollte doch was passieren, gilt es, mit Bedacht vorzugehen.

Der Autor
Roman Stefanov
Cybersecurity-Verantwortlicher,
Cisco Schweiz

Längst hat sich eine Gegenwirklichkeit zur Internetwirtschaft entwickelt, die nach ähnlichen Gesetzmässigkeiten funktioniert: Die organisierte Kriminalität im Netz verhält sich kaum anders als ein E-Commerce-Konzern. So wie es von fast jedem Superhelden eine böse Version gibt, sind auch im Darknet, dem Untergrund des Internets, die Mechanismen der Marktwirtschaft nicht ausser Kraft gesetzt. Der jüngste Schrei ist Ransomware-as-a-Service (RaaS): Ganz ohne Hackerkenntnisse lassen sich hiermit Unternehmen und andere Ziele im Internet attackieren und Lösegelder für verschlüsselte Daten erpressen.

2021 haben die Ransomware-Attacken stark zugenommen, nicht zuletzt wegen bequemer und einfacher Dienste, die man bei Kriminellen mietet. Die Wachstumsraten sind zweistellig, und laut diverser Quellen wird inzwischen der Grossteil solcher Angriffe mit RaaS ausgeführt, bei dem die Angreifer eine gemietete Infrastruktur und erprobte Taktiken nutzen und einen gewissen Prozentsatz der Lösegelder an den RaaS-Betreiber abführen. Ein neues Allzeithoch an Datendiebstählen prognostiziert das neutrale Identity Theft Resource Center (ITRC) für die USA. Gleichzeitig sind laut ihm immer weniger Menschen individuell davon betroffen. Dafür Organisationen. In den letzten zwei Jahren haben laut der «Cisco Security Outcomes Study – Endpoint Edition» weltweit mehr als 40 Prozent einen erheblichen Sicherheitsvorfall oder Datenverlust erlebt.

Das Datendilemma

Heute arbeiten immer mehr Menschen mit Videokonferenz- und Collaboration-Software ausserhalb des Firmenperimeters. Die Homeoffice-Arbeitsplätze mit neuen Angriffsflächen und ungesicherten Schnittstellen – vor allem RDP-Servern – tragen das Ihre zur schnelleren und leichteren Verbreitung von RaaS-Attacken bei. Die Augen davor zu verschliessen, hilft nicht: Jeder Mitarbeitende und jedes Unternehmen, das seine Infrastruktur, Netzwerke und Daten nur ungenügend schützt, erhält die Systeme der organisierten Kriminalität am Leben.

Vielleicht hilft es, einen Schritt zurückzutreten und das grosse Bild zu betrachten: Jede Art von Daten ist interessant für Hacker. Fast alles lässt sich zu Gold – im Darknet zu einer Kryptowährung – machen. Mit mehr oder weniger drastischen Auswirkungen für die Eigentümer der Daten. Beispielsweise Clubhouse: Der zu Beginn dieses Jahres viel Aufmerksamkeit zuteil gewordenen Social-Media-App sind 3,8 Milliarden Telefonnummern gestohlen worden, allesamt zuvor beim Synchronisieren der Smartphone-Telefonbücher eingesammelt. Bereits im Frühling wurde der Diebstahl von 1,3 Millionen Datensätzen über die Social-Media-Verbindungen der Clubhouse-Nutzer bekannt, öffentlich zugängliche Profilinformationen, abgesaugt über die Datenschnittstelle und im Darknet verkauft. Auf eine ähnliche Art und Weise wurden jüngst auch 500 Millionen Linkedin-Daten abgegriffen. Zwei scheinbar harmlose Beispiele. Sie zeigen die Dimensionen: Die organisierte digitale Kriminalität verwertet jedes Datenbit. Mit den Clubhouse-Telefonnummern beispielsweise sind präzise Phishing-Kampagnen möglich, die später zu eigentlichen Hacks führen.

Ein Dilemma: Ohne Daten kein Internet und keine Digitalisierung. Ohne Cloud Computing keine Business-Resilienz. Es braucht neue Sicherheitsansätze, ja eine Sicherheitskultur, um das Problem in den Griff zu bekommen: Wer sich seiner Daten bewusst ist, wird sie besser zu schützen wissen. Jedoch sind laut PWC weniger als die Hälfte aller Unternehmen global auf Attacken vorbereitet; laut Cisco-Studien ist das Thema inzwischen im Top-Management angekommen. Kein Wunder: Laut dem «Cybersecurity Almanac» von Cybersecurity Ventures ist das Geschäft mit gestohlenen Daten deutlich lukrativer als der illegale Drogenhandel. Und weitaus risikofreier.

Was alles in Gefahr ist

Die organisierte digitale Kriminalität handelt mit allem was nicht niet- und nagelfest ist, von Telefonnummern bis zu kompletten Kreditkartendatensätzen, vom Cookie bis zu geprüften Logins. Die interessanten Daten lassen sich in drei Kategorien einteilen: Geschäftsgeheimnisse, personenbezogene Daten und Daten, die Aufschlüsse über die Arbeitsroutinen geben. Ihr Handel im Darknet, bei regelrechten Auktionen teilweise, bei geschäftlichen Transaktionen mit Garantieservice (veraltete Daten werden kostenlos ausgetauscht), führt zu verschiedenen Formen der Kriminalität im realen Leben – mehr Spam ist noch die harmloseste.

Geschäftsgeheimnisse werden verkauft, personenbezogene Daten für verschiedene Kampagnen genutzt, beispielsweise für

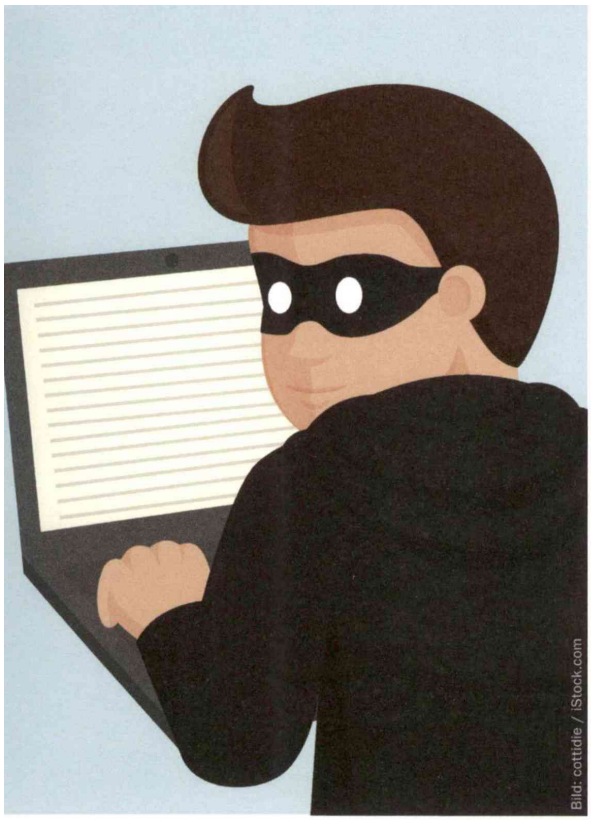
Bild: cottidie / iStock.com

Phishing oder Scam-Attacken. Mit Passwörtern einer Website lassen sich leicht auch andere Services knacken, denn kaum jemand verwendet für jeden Internetservice unterschiedliche Passwörter. Auf diese Weise lassen sich auch indirekte Attacken reiten, über die Websites von Zulieferern etwa, wie es jüngst die «REvil»-Akteure im Kaseya-Fall vorgemacht haben. Wer weiss, wie die Mitarbeitenden in Firmen und IT-Abteilungen ticken, kann sich als einer der Ihren ausgeben und sich so ins Netzwerk einschleichen. Oder sich im Namen des CEO Geld überweisen lassen. Wenn die Daten Einblicke in die Sicherheitsvorkehrungen einer Firma geben, lässt sich vielleicht ein physischer Einbruch planen. Generell sind Daten jeder Art unter Umständen hilfreich bei der Vorbereitung grösserer Angriffe.

Die Marktplätze für gestohlene Daten funktionieren kaum anders als legale E-Commerce-Angebote, sie verfügen gar über eigene Compliance-Strukturen. Nur eben anonym und illegal. Dabei lässt sich mit Bewertungen einschätzen, ob man für seine Vorauszahlung für die Daten jemals einen Gegenwert erhält. Einen kompletten Kreditkartendatensatz gibt's etwa für 25 US-Dollar.

Seit Beginn der Pandemie haben sich die Umsätze im Darknet laut Schätzungen stark vergrössert, laut dem «Dark Web price Index 2021» von Privacy Affairs greifen auch Marktgesetze wie Angebot, Qualität und Nachfrage. Übrigens operieren die Kriminellen nicht ausschliesslich im Verborgenen. Ciscos Talos-Forscher haben bereits 2019 mehr als 70 Gruppen mit fast 400 000 Mitgliedern auf Facebook identifiziert, in denen Informationen und Tools ausgetauscht werden.

Was zu tun ist

280 Tage dauert es laut Ponemon-Studien im Industriedurchschnitt, bis ein Datendiebstahl überhaupt bemerkt wird. Nur etwas mehr als die Hälfte der Alarme werden überhaupt angeschaut und weniger als die Hälfte davon überhaupt behoben. Und wenn mal ein System ausfällt, dauert es laut einem globalen Report von Veeam in der Schweiz 71 Minuten bis zur Wiederherstellung.

Sicher ist: Je länger es dauert, bis die Ursachen eliminiert sind, desto teurer wird's. Oft bemerkt man den Hack erst, wenn man offen bedroht wird: zu spät. Es ist Eigenverantwortung, etwas zu unternehmen, bevor überhaupt eine Attacke wirksam wird. Und es ist verantwortungsvoll, wenn nach einer Attacke nicht reflexartig gezahlt und in der Cybersecurity Business as usual betrieben wird, sondern an das ganze System gedacht wird. Die organisierte digitale Kriminalität lebt von Unternehmen und IT-Mitarbeitenden, die Cybersecurity auf die lange Bank schieben, weil ja normalerweise nichts passiert.

Sobald eine Attacke entdeckt wird, gilt es, auf technischer und organisationeller Ebene (siehe Kasten) die nötigen Massnahmen einzuleiten. Das revidierte Datenschutzgesetz, das im Laufe von 2022 in Kraft treten wird, sieht zudem eine Meldepflicht beim Eidgenössischen Datenschutzbeauftragten vor, wenn Verletzungen der Datensicherheit die Persönlichkeit oder Grundrechte von Menschen in hohem Masse beeinträchtigen.

Die wichtigste Massnahme in Unternehmen ist es, sich nicht länger auf einzelne Gefahren zu fokussieren, sondern eine Sicherheitskultur zu etablieren, die unabhängig vom Arbeitsort ihre Wirkung entfalten soll. Wir müssen schlicht mit Attacken leben lernen und sie mit einer klugen Mischung aus Technologie (etwa mit künstlicher Intelligenz im Netzwerk, die Anomalien erkennt und einer Zero-Trust-Architektur) und sicherem Verhalten und vorausschauenden Analysen (Threat Hunting) ins Leere laufen lassen. Dazu zählt auch die unternehmerische und persönliche Haltung, seine Daten so zu schützen, dass wir nicht unbeabsichtigt das Geschäftsmodell der organisierten digitalen Kriminalität am Leben erhalten.

MASSNAHMEN

So sollte eine Firma im Fall von Datenverlust reagieren

Sind Daten abgeflossen, gibt es einiges zu tun. So ist auf der technischen Ebene zu klären, was genau geschehen ist, welche Daten betroffen sind und dann die Lücken zu schliessen. Zudem gilt es, die Kommunikation festzulegen: Wer muss was wissen? Das NCSC empfiehlt die proaktive Information der Kunden. Je nach Risikoeinschätzung gilt es zudem, den Eidgenössischen Datenschutzbeauftragten via edoeb.admin.ch zu informieren. Spezifischere Informationen über die Massnahmen nach einem erfolgreichen Angriff finden sich im NIST-Framework und in der EU-DSGVO. Das Nationale Zentrum für Cybersicherheit der Schweiz bietet eine umfangreiche Checkliste für CISOs.

Den vollständigen Artikel finden Sie online
www.netzwoche.ch