STORMSHIELD

MEINUNGEN

WELCHE TENDENZEN ZEICHNEN SICH FÜR DIE CYBERSICHERHEIT 2022 AB?

Victor Poitevin
Editorial & Digital Manager, Stormshield

Es überrascht nicht, dass das Jahr 2021 in Bezug auf Cyberbedrohungen besonders intensiv war. Der öffentliche Sektor (Gesundheitswesen und Kommunen) kommt nicht zur Ruhe, Ransomware weitet sich auf größere Ziele aus (Colonial Pipeline, JBS Food ...) oder die Bedrohungen rund um den Datenschutz mit der Spionagesoftware Pegasus: alles Beispiele für ein Jahr wie kein anderes, mit der Schwachstelle Log4Shell zu Weihnachten ... Was ist also in Bezug auf Cyberbedrohungen im Jahr 2022 zu erwarten? Vorausschauende Übung, mit unseren vier Prognosen zur Cybersicherheit für das Jahr 2022.

Wenn das Jahr der Cybersicherheit 2021 in einem Trend zusammengefasst werden müsste, wäre es der Trend zu einer Strukturierung auf Seiten der Cyberkriminellen. Parallel zur Explosion der Fälle und der Beträge konsolidiert sich das Ökosystem der cyberkriminellen Gruppen zu einer regelrechten Schattenwirtschaft mit dem erklärten Ziel, die Rentabilität der Angriffe zu verbessern. Sie war jedoch nicht das einzige starke Signal, das das vergangene Jahr bewegte. Welche Lehren lassen sich aus 2021 ziehen? Welche Bedrohungen könnten im Jahr 2022 entstehen? Wie jedes Jahr stellen wir uns dem Spiel der Prognosen.

TREND 1: AUF DEM WEG ZUR HYPERPROFESSIONALISIERUNG VON CYBERKRIMINELLEN?

Die (nicht ganz so schwachen) Signale von 2021

Im Jahr 2021 haben die Gruppen der Cyberkriminellen einen Meilenstein in ihrer Strukturierung erreicht. Das Ökosystem der Ransomware beruht beispielsweise auf einer Vielzahl von Akteuren, von Entwicklern bis hin zu Wiederverkäufern von Zugängen oder Daten. Es haben sich regelrechte Plattformen gebildet, die auch auf Mitglieder zurückgreifen, um ihre niederen Werke zu verrichten. So hat sich der Trend zu *Ransomware as a Service* (RaaS) erheblich verstärkt im Jahr 2021. Und diese Industrialisierung ruft die Experten auf den Plan. „*Die Cyberkriminellen schaffen eine Art ERP für Cyberangriffe mit Plattformen, die die Werkzeuge, die angegriffenen Kunden, die Kundendienstchats, die Lösegeldzahlungen usw. verwalten*", alarmierte beispielsweise Gérôme Billois, Partner für Cybersicherheit und digitales Vertrauen bei Wavestone, bei einer Veranstaltung in Frankreich. *Wir haben es mit einem Ökosystem zu tun, das eine Größenordnung erreicht hat, die es auch gewöhnlichen Cyberkriminellen ermöglicht, anzugreifen. Sie gehen sogar so weit, dass sie in ihren Foren eine Art Schiedsgericht einrichten, wenn es zu Zahlungsausfällen zwischen der Plattform und dem Cyberkriminellen kommt.*"

Auch im Jahr 2021 gab es eine Reihe von Polizeieinsätzen gegen diese Gruppen von Cyberkriminellen. Diese staatlichen Reaktionen, die von der internationalen Zusammenarbeit geprägt waren, waren bis dahin sehr selten. Im Jahr 2021 sind jedoch zwei wichtige Episoden zu verzeichnen: die der Zerschlagung des Botnets Emotet und die der Zerschlagung der Ransomware-Gruppe REvil. Ein Anfang für eine Regulierung? Schwer zu sagen, da die zerschlagenen Operatoren dazu neigen, sich dahinter schnell neu zu formieren oder sich sogar rekrutieren zu lassen ... So wurden zwischen September und November 2021 drei neue cyberkriminelle Gruppen identifiziert: Lockean, FamousSparrow und Void Balaur. Schlagt einen Kopf ab, und drei weitere wachsen nach ...

Und auf der hellen Seite der Macht ist der Trend für 2021 immer noch ein Mangel an Fähigkeiten und Talenten. Während in Frankreich bis 2021 700.000 zusätzliche Stellen besetzt wurden, weist der Bereich der Cybersicherheit noch immer ein Defizit von 65 % bei den Arbeitskräften, nach Zahlen von Microsoft. Allein in den USA soll ein Drittel der Arbeitsplätze im Bereich der Cybersicherheit unbesetzt bleiben.

Das Szenario 2022

Auf dem Weg zu einem Transfermarkt für Cyberkriminelle? Es ist fast schon beschlossene Sache, dass im kommenden Jahr eine oder mehrere neue Gruppen von Cyberkriminellen auftauchen werden. Doch mit der chronischen Vermehrung der Gruppen und ihrer Strukturierung wird sich die gleiche Frage stellen wie bei den Fachleuten für Cybersicherheit: die Frage nach der Rekrutierung von Talenten. Im Cyberbereich, wo Hackertalente rar sind, könnte der Wettbewerb durchaus zu einer Rekrutierungspolitik führen, die seitens der Gruppen von Cyberkriminellen viel aggressiver werden. Wie in der Sportwirtschaft könnten in Zukunft Agenten entstehen, die ihre Schützlinge an die meistbietenden Gruppen vermitteln. Agenten, die nicht zögern würden, neue Methoden einzuführen, wie z. B. Prämien für die Unterzeichnung von Verträgen oder „Ausleihen" zwischen Gruppen.

TREND 2: AUF DEM WEG ZU NOCH RAFFINIERTEREN CYBERANGRIFFEN?

Die (nicht ganz so schwachen) Signale von 2021

Auf der Bedrohungsseite haben die Angriffe durch Ransomware um 62 % zugenommen und im Jahr 2021 die Medien weitgehend beherrscht. Aber auch andere Verfahren haben sich entwickelt, darunter der Lieferkettenangriff (oder *supply chain attack*). Paradebeispiel des Jahres ist das Unternehmen Codecov, das eine Software zur Prüfung von Quellcode herausgibt, einen Cyberangriff im April 2021. Durch die Kompromittierung seiner Software konnten Cyberkriminelle Hunderte von Kundennetzwerken infiltrieren.

Eine weitere Art von Angriff, die sich zu noch mehr Subtilität entwickelt, ist die Spionagesoftware. Im Juli 2021 wurde das aufsehenerregende „Projekt Pegasus" enthüllt, ein weltweites System zum Ausspionieren der Smartphones von Journalisten, Anwälten, Aktivisten und Politikern. Insgesamt wurden über 50.000 Telefonnummern potenzieller Ziele von Amnesty International und dem Ermittlungskonsortium Forbidden Stories identifiziert.

Und eine neue Schwachstelle sorgte 2021 für Schlagzeilen. Verbunden mit der Open-Source-Bibliothek Log4j und mit dem Namen Log4Shell. Diese *Zero-Day-Sicherheitslücke* hat Panik ausgelöst. Im Dezember 2021 schloss die Regierung von Québec auf diese Weise präventiv 4000 Regierungswebsites, um Angriffe zu vermeiden. Im selben Monat berichteten die Cybersicherheitsteams von Microsoft, dass Lösegeldangriffe auf *Minecraft-Server* gerichtet waren, die von Nutzern des beliebten Videospiels gehostet wurden. Ein *Modus Operandi*, der die Anfälligkeit von Anwendungen verdeutlicht, da viele von ihnen auf bereits existierenden Code-Bausteinen beruhen, die nicht unbedingt sehr robust sind und nur selten vor ihrer Verwendung evaluiert wurden ...

Das Szenario 2022

Auf dem Weg zu einer Explosion von Zero-Day-Schwachstellen, die in Open-Source-Bibliotheken versteckt sind? Die Macht des Log4Shell-Angriffs könnte (leider) morgen mehr als eine Gruppe von Cyberkriminellen inspirieren. Denn das Funktionieren des Systems der freien Software selbst bringt es mit sich, dass große Teile des Internets von einer Handvoll Freiwilliger gepflegt werden. Wenn große Unternehmen morgen nicht in die von ihnen genutzten Open-Source-Projekte investieren, können die Patches nicht mit der Geschwindigkeit der Entdeckung kritischer Schwachstellen Schritt halten. Und Cyberkriminelle könnten dann problemlos besonders sensible Infrastrukturen, Netzwerke oder Daten angreifen. Zum Beispiel in Frankreich auf die in der Anwendung TousAntiCovid enthaltenen Strukturen. Durch das Erkennen einer Schwachstelle in den veröffentlichten Codeteilen, könnte die 2021 am häufigsten heruntergeladene Anwendung den Cyberkriminellen die Möglichkeit bieten, auf eine riesige Menge an Gesundheitsdaten und Gesundheitspässen zuzugreifen. Mitten in den Präsidentschaftswahlen wären die politischen Auswirkungen eines solchen Cyberangriffs nicht zu unterschätzen.

TREND 3: DAS ENDE DES MEDIALEN LUPENEFFEKTS?

Die (nicht ganz so schwachen) Signale von 2021

Colonial Pipeline, JBS Food, Log4Shell: All diese Cyberangriffe sorgten im Jahr 2021 für Schlagzeilen. Sehen Sie nicht den Zusammenhang zwischen ihnen? Suchen Sie nicht im Cyberspace, denn ihre einzige Gemeinsamkeit ist der Medienrummel, den sie ausgelöst haben. Ein mediales Lupenphänomen, das zu einem falschen Sicherheitsgefühl bei Kleinst- und Kleinunternehmen führen kann. Laut einer internationalen Studie von Forrester Consulting, die im Januar 2021 veröffentlicht wurde, beträgt der Anteil der von Cyberangriffen betroffenen Klein- und Mittelbetriebe mit weniger als 250 Mitarbeitern jedoch 33 %. Der Medienfokus ist also selektiv: Wer hat schon von Cyberangriffen auf die Anwaltskanzlei, die Wirtschaftsprüfer oder gar den Klempner an der Ecke gehört? Und die Größe spielt kaum eine Rolle, da auch größere Unternehmen unter dem Radar der Medien fliegen. Im Februar 2021 wurde beispielsweise der Bootshersteller Bénéteau von einem groß angelegten Cyberangriff getroffen, ohne die Massen zu bewegen, obwohl 3.900 Mitarbeiter betroffen waren. Eine weitere potenzielle Folge des Medien-Lupeneffekts ist ebenfalls hervorzuheben: Ein großer Medienrummel kann dazu führen, dass Gruppen von Cyberkriminellen, die immer darauf aus sind, neue Opfer zu finden, die wenig oder schlecht gesichert sind, neue Ziele finden.

Ein weiteres (nicht ganz so schwaches) Signal war im Februar 2021 zu vernehmen, als der Videospielverlag CD Projekt Opfer von Ransomware wurde, und zwar kurz vor der Veröffentlichung eines neuen Spiels, das im Cyberpunk-Universum angesiedelt war. Ein Augenzwinkern und vor allem eine neue Episode nach Capcom und Electronic Arts, die in den vergangenen Jahren Opfer waren. Denn die großen Herausgeber und Studios von Videospielen sind schon jetzt beliebte Ziele für Cyberkriminelle. Doch während bislang vor allem Reputationsschäden die Folge waren, könnte sich das Blatt (schnell) wenden.

Tatsächlich kündigte Facebook Ende Oktober 2021 mit großem Tamtam die Einführung virtueller Welten als nächste Welle des Internets und logische Fortsetzung der Online-Videospiele an. Und das schnelle Überschlagen: Grundstückskäufe im Wert von über einer Million Dollar wurden bereits innerhalb dieses virtuellen Universums getätigt.

Das Szenario 2022

„Metaversum-Polizei, NFT bitte“. Beliebtheit, Medienfokus und hohe Geldbeträge; diese virtuellen Welten könnten zum neuen bevorzugten Spielfeld von Cyberkriminellen werden. Und ihre Hauptmotivation wäre natürlich weiterhin das Geld. Vom Lösegeld für digitale Artefakte, die für horrende Summen gekauft wurden, bis hin zum Diebstahl von NFT – die kriminellen Möglichkeiten sind vielfältig. Die Herausgeber von virtuellen Welten oder Online-Spielen könnten schnell von Wellen von Cyberangriffen überrollt werden, die die Entwicklung ihrer Produkte beeinträchtigen. Eine Metaversum-Polizei, die sich auf eigene Ermittlungsinstrumente stützt, würde dann notwendig werden. Sie würde Experten aus der ganzen Welt zusammenbringen, deren Ziel es wäre, Cyberkriminelle in den entlegensten Winkeln des Metaversums aufzuspüren. Eine Herausforderung, da die Transaktionen innerhalb ihrer Räume im Laufe des Jahres massiv ansteigen werden.

TREND 4: AUF DEM WEG ZUR CYBERSICHERHEIT FÜR ALLE?

Die (nicht ganz so schwachen) Signale von 2021

Auch 2021 bleibt der Mensch das wichtigste Tor zum Netzwerk eines Unternehmens. Laut einer IDG-Studie haben 44 % der großen Unternehmen (500-999 Mitarbeiter) in diesem Jahr Netzwerkunterbrechungen von mehr als einem Tag aufgrund von Phishing-Angriffen erlitten, verglichen mit 14 % der kleinen Unternehmen (25-100 Mitarbeiter). Und die neuesten verfügbaren Zahlen besagen, dass im Jahr 2021 22 % der gemeldeten Datenverletzungen mit einer Phishing-E-Mail begannen.

Ein Viertel der französischen Arbeitnehmer arbeiteten im Jahr 2021 mindestens einen Tag pro Woche im Homeoffice. Da wird die Frage der Zugänglichkeit von Cybersicherheitslösungen (weltweit) noch wichtiger: Mitarbeiter nutzen ihre Firmengeräte auch für private Zwecke und vervielfachen damit potenzielle Einfallstore.

Und das Bewusstsein für digitale Hygiene und Cybersicherheit ist noch ein langer Weg. Nach dem Bericht 2021 des US-amerikanischen Unternehmens KnowBe4 glaubt ein Viertel der Beschäftigten, dass das Anklicken verdächtiger Links oder Anhänge ein geringes oder gar kein Risiko birgt. Da möchte man mit dem Kopf gegen die Wand rennen ...

Das Szenario 2022

Auf dem Weg zu einem individuellen Cyber-Score für Mitarbeiter? Am 22. November 2022 klickt Jeanine, eine Chefsekretärin in einem großen Haushaltsgerätekonzern, auf einen Link in einer E-Mail, in der ihr mitgeteilt wird, dass sie das neueste iPhone gewonnen hat. Einige Tage später gelingt es der IT-Abteilung des Unternehmens nach tagelangem Kampf, den Ransomware-Cyberangriff auf das Computernetzwerk des Unternehmens einzudämmen. Nach einer kurzen Untersuchung wird Jeanine von der Personalchefin vorgeladen: Ihr wird mitgeteilt, dass ihr Punkte auf ihrem persönlichen Cyber-Score abgezogen werden. Seit einigen Monaten haben sich einige Unternehmen tatsächlich dazu entschlossen, dieses System einzuführen, das ihren Mitarbeitern ein besseres Verständnis dafür vermittelt, dass Cybersicherheit alle angeht. Jeder hat ein Startguthaben, das bei Verfehlungen sinkt oder nach Schulungen oder wenn gute Praktiken eingeführt werden, steigt. So sieht Paul, Manager eines Teams von Vertriebsmitarbeitern, seinen Cyber-Score steigen, nachdem er eine Endpoint-Lösung auf den Laptops seiner mobilen Mitarbeiter installieren lässt. Und wehe dem leitenden Angestellten, der die Fußballspiele seiner Lieblingsmannschaft auf illegalen Streaming-Websites verfolgt ...

Solche Szenarien und Zukunftsvisionen **könnten sich bereits 2022 realisieren** – wir sollten sie aufmerksam verfolgen.