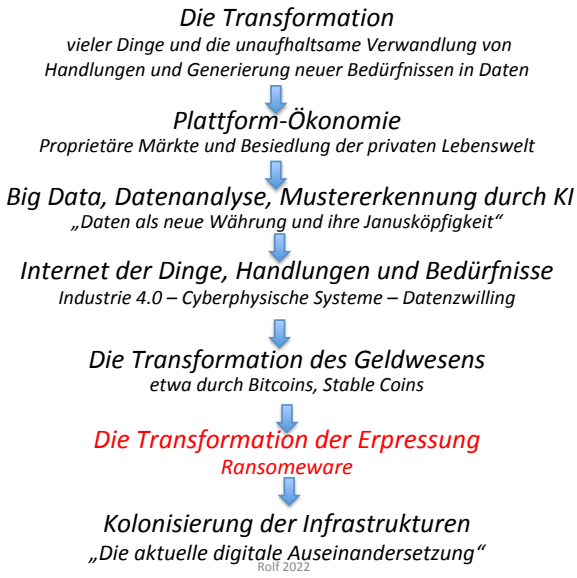
Die Transformation der Erpressung - Ransomware



Entstofflichung der Assets

Ein wesentliches Merkmal der digitalen Transformation ist die Virtualisierung physischer Gegenstände, aber auch der Interaktionen unseres Alltags. Diese werden nun in Daten abgebildet. Daher steigt auch die Anzahl der entstofflichten Wertgegenstände und Dienstleistungen stetig und es liegen zunehmend mehr Assets (wertvolle Dinge, nicht zwingend physische Gegenstände [1]) bzw. wertvolle Informationen in digitaler Form vor.

Private Bilder werden in der Cloud gespeichert; persönliche Nachrichten werden nicht mehr in Form von Briefen verschickt, sondern digital über den Messenger des Vertrauens. Natürlich wird eine Sicherung des Chatverlaufs sicherheitshalber ebenfalls in einer Cloud gespeichert. Quasi jeder Mensch, der sich in der digitalisierten Welt von heute bewegt, besitzt und/oder generiert sensible Daten, die in digitaler Form hinterlegt sind.

Auch andere Assets, wie beispielsweise der Zugriff auf das eigene Bankkonto oder auf das Auto finden heute digital statt; es ist bereits heute durchaus möglich, ein Bankkonto zu eröffnen und zu führen, ohne jemals in eine physische Bank zu gehen oder mit einem Menschen zu interagieren. Ein Auto kann mittlerweile mit einem rein digitalen Schlüssel entsperrt und gefahren werden.

Diese Entstofflichung der Assets betrifft jedoch nicht nur Privatpersonen. Auch unternehmensinterne Assets liegen zunehmend in digitaler Form dar, da zunehmend mehr Dienstleistungen digital erbracht werden. Die Arbeit, die beispielsweise ein Ingenieursbüro an einem Arbeitstag erbringt, wird als Daten auf den Servern des Unternehmens gespeichert. Erbringt es keine Arbeit in digitaler Form, so hat heutzutage dennoch so gut wie jedes Unternehmen digitale Assets wie Datenbanken, in denen Kundeninformationen hinterlegt werden und welche für den Betrieb elementar wichtig sind. Aber auch viele physische Prozesse, etwa die Steuerung von Produktionsanlagen, geschehen heute digital; somit ist hier allein der Zugriff auf diese Systeme wertvoll, die Daten eher weniger.

Allgemein können daher heutzutage vier Klassen digitaler Assets unterschieden werden, die für diesen Essay relevant sind:

1. Emotional behaftete Daten, etwa Bilder von Verstorbenen
2. Sensible Daten, etwa Bewegungsprofile oder Unternehmensgeheimnisse
3. Kritisch benötigte Daten, etwa Arbeitsfortschritte
4. Digitaler Zugriff auf wertvolle Ressourcen, etwa das eigene Auto oder eine Steuerungsanlage

Transformation der Erpressung

Da nun zunehmend mehr wertvolle Daten in digitaler Form existieren, hat sich auch die Kriminalität, insbesondere die Subdomäne der Erpressungskriminilatität, daran angepasst. Dies ist eine durchaus logische Entwicklung: dort wo die Assets sind, findet auch die Erpressung statt, gerade wenn dies opportun ist.

Heutzutage ist kein physischer Einbruch oder eine Androhung von Gefahr für Leib und Leben nötig, um Personen oder Unternehmen zu erpressen. Auch Lösegeldzahlungen sind aufgrund der Entstofflichung des Geldes [2] (noch) problemlos anonym realisierbar. Mittels digitaler Währungen wie Bitcoin bleibt die Identität der Täter oft unerkannt (digitale Erpressung war zwar auch vor der Einführung dieser präsent, erforderte aber einiges an Know-How im Bereich der Geldwäsche).

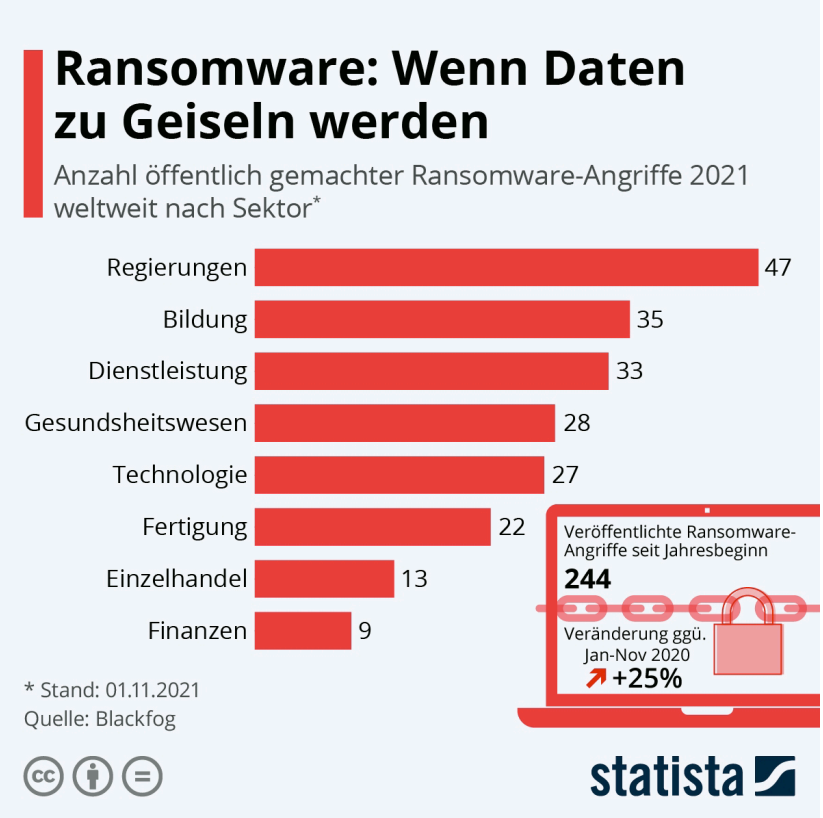
Erleichternd kommt hinzu, dass es Staaten (vor allem in der ehemaligen UdSSR) gibt, in denen meist nur dann gegen enttarnte Täter vorgegangen wird, wenn diese auch im eigenen Land aktiv waren. Wer also sorgsam genug in seiner Opferauswahl ist und nicht in Staaten mit den falschen Auslieferungsabkommen reist, kann davon ausgehen, straffrei zu bleiben. Dass diese Entwicklungen das Risiko für die Täter

deutlich verringert, ist ein weiterer Grund für die zunehmende Digitalisierung der Erpressung.

Einsatz von Ransomware

Als Ransomware bezeichnet man Erpressungssoftware, welche in das Netzwerk bzw. auf das Gerät des Opfers eingeschleust wird und so mit diesem interagiert. Damit ist die Voraussetzung geschaffen, ein Lösegeld (engl. „ransom“) fordern zu können. Mithilfe einer solchen Software wird häufig der Zugriff des Opfers auf die eigenen Daten bis hin zum ganzen Netzwerk unmöglich. Dabei werden die Daten in der Regel verschlüsselt, um für die Entschlüsselung ein Lösegeld zu verlangen.

Der durch einen solchen Angriff entstandene Schaden kann durch rechtzeitige Backups verringert werden. Sichert ein Unternehmen beispielsweise am Ende jeden Tages den gesamten Datensatz (Voll-Backup), so können die Datenserver im Fall einer böswilligen Verschlüsselung der Daten auf den Stand des letzten Backups zurückgesetzt werden. Daher versuchen Täter oft, die Backupsysteme ebenfalls unbrauchbar zu machen oder leiten oft zusätzlich die sensiblen Kunden- und Unternehmensdaten aus dem System heraus und drohen mit deren Veröffentlichung (sogenannte „double extortion“). Teilweise werden auch Kunden oder Unternehmenspartner kontaktiert, um den Druck auf das Opfer zu erhöhen [3].



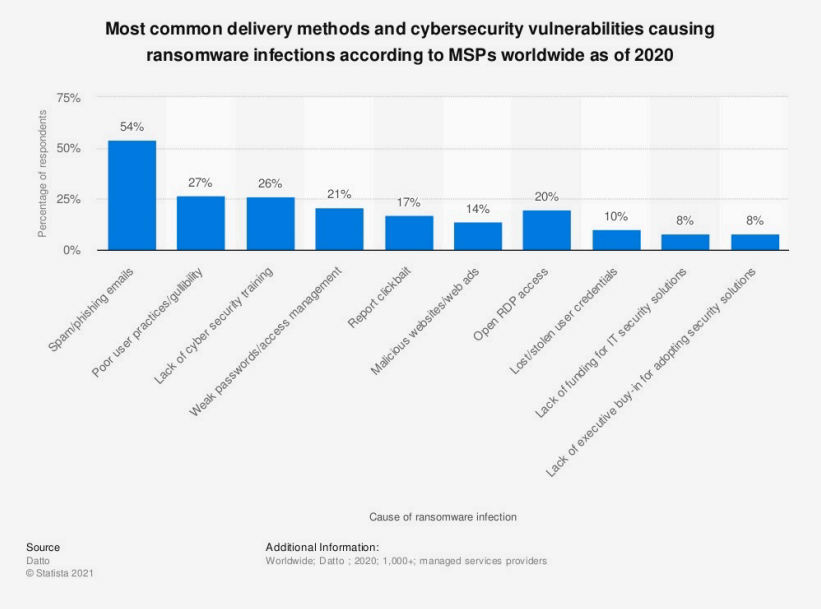
Quelle: htt p s://de.statista.com/infografik/26162/anzahl-oeffentlich-gemachterransomware-angriffe-2021

Während Ransomware anfänglich auch oft Privatpersonen betraf, (vermutlich da diese tendenziell schlecht geschützt waren und eine intensive Strafverfolgung inklusive Nachverfolgung der Geldströme unwahrscheinlich schien), sind in den letzten Jahren neben Unternehmen auch zunehmend Behörden ins Ziel der Angreifer geraten. Während bei Privatpersonen a) wenig Lösegeld zu holen ist und b) tendenziell weniger wertvolle digitale Assets vorliegen, ist dies bei Unternehmen und Behörden anders. So war beispielsweise der Landkreis Ludwigslust-Parchim aufgrund eines Ransomware-Angriffs vor kurzem monatelang im Notbetrieb und nicht in der Lage die meisten Dienstleistungen zu erbringen, geschweige denn die aktuellen Covid-Zahlen zu melden [4].

Wie der obigen Grafik zu entnehmen ist, machen Regierungs- und Bildungsinstitutionen den Löwenanteil der zwischen Januar und November 2021 weltweit gemeldeten Ransomwarefälle aus. Hier ist allerdings anzumerken, dass gerade diese Branchen in der Regel dazu verpflichtet waren, diese auch zu melden, während Wirtschaftsunternehmen Motive hatten, dies nicht zu tun (etwa um Anleger nicht zu verunsichern). Die eigentliche Zahl der Vorfälle ist also wahrscheinlich um einiges höher und die Aufteilung dieser weniger in Richtung öffentlicher Institutionen verteilt.

Der Weg ins System

Zugang zum System erhalten Täter meist auf den traditionellen Schadsoftwarewegen: mithilfe von Phishingmails, Sicherheitslücken in Hard- oder Software (vor allem dem Remote-Desktop-Protocol) oder durch fahrlässige Verwendung von unbekannten Datenträgern (z.B. USB-Sticks) am System. In den letzten Jahren ist aber auch ein weiterer Angriffsvektor hinzugekommen: Managed Service Providers, kurz MSPs. Diese verwalten die Systeme von Unternehmen, die sich kein eigenes Personal in dem Bereich leisten wollen/können oder derart generische Systeme verwenden, dass es Sinn macht, diese von einem damit vertrauten Dienstleister verwalten zu lassen. Da MSPs quasi ausschließlich Unternehmen, also generell lukrative Ziele als Kunden haben, sind sie zum Ziel zahlreicher (teils erfolgreicher) Angriffe geworden. So wurde 2021 etwa der amerikanische MSP Kaseya das Opfer eines Angriffs der Ransomware-Gruppe REvil, die mithilfe der Kaseya-Zugänge die Systeme von zahlreichen Unternehmen verschlüsselten, u.a. die Kassensysteme der schwedischen Supermarktkette coop [5].



Quelle: https://www.statista.com/statistics/700965/leading-cause-of-ransomwareinfection/

Der beigefügten Grafik ist zu entnehmen, dass schadhafte Emails noch immer den mit Abstand größten Angriffsvektor darstellen, vor allem da diese in einigen anderen genannten Gründen, welche sich auf das Nutzerverhalten als Ursache konzentrieren, durchaus mitgemeint sein können.

Aber auch das Thema Access Management scheint eine große Schwachstelle vieler Unternehmen zu sein. Wer (gerade in Zeiten der Covidpandemie) per VPN-Zugängen die Arbeit von zuhause aus ermöglicht, sollte diese Zugänge auch gut sichern, etwa per Multi-Faktor-Authentifizierung. Andernfalls reicht ein leicht zu knackendes Passwort, um Zugang zu erhalten.
Eine wichtige Sicherheitslücke, deren Ausnutzung in der Regel keiner Nutzerinteraktion bedarf, scheint auch weiterhin das RDPProtokoll bzw. eine Miskonfiguration von diesem zu sein. Eine Schwachstelle in diesem Protokoll ermöglichte Wannacry, den wohl bekanntesten Ransomware-Wurm (ein durchaus seltener Verbreitungsweg von Ransomware).

Vermutlich ist der Weg über einen infizierten MSP nicht aufgelistet, da hier zum einen MSPs befragt wurden (diese haben in der Regel einen guten Überblick über die Situation aber selbstverständlich wenig Interesse daran, sich selbst als Einfallstor zu nennen) und zum anderen im Jahr 2020 dieser Weg sowieso noch nicht sonderlich verbreitet schien.

Ransomware as a Service

Nicht nur das Risiko für den Täter hat sich aufgrund der Digitalisierung verringert, sondern auch der Aufwand. In einschlägigen Foren hat sich die digitale Erpressung professionalisiert und Interessierte können Erpressungssoftware wie einen Service nutzen. Die „Profis“ vollführen jedoch nicht

den Angriff für den Nutzer des Service; Anbieter und Betreiber stellen lediglich die Ransomware zur Verfügung, wickeln die Lösegeldzahlung ab und führen die Übergabe der Entschlüsselungsinformationen durch oder überlassen gar alles außer der Software anderen Dienstleistern [6]. Nutzer eines solchen Service haben oft die Möglichkeit ein monatliches Abonnement zu nutzen oder eine einmalige Gebühr für den Service zu zahlen. Auch findet man Partnerschaftsmodelle: der Betreiber erhält einen festen Prozentsatz jeder Lösegeldzahlung der Opfer. Durch einen solchen Service sinkt die „Barrier of entry“ der Erpressung: Täter müssen nun lediglich den Zugang zum System schaffen, wobei es auch hierfür bereits Services gibt.

Dies ist vergleichbar zum Software-as-a-Service Modell, welches sich zunehmend in der Geschäftswelt durchsetzt. Der Kunde hat hier ebenfalls den Vorteil, dass zur Software die Infrastruktur und die dazugehörige Wartung gleich mitgeliefert wird, während das Softwareunternehmen den Vorteil hat, dass die Lizenzierung wesentlich einfacher und lukrativer ist, da auch mit Infrastruktur und Wartung Profit gemacht werden kann.

Digitale Transformation verstehen, Herausforderungen erkennen

Technische Kenntnisse zum Erstellen von Schadsoftware sind nicht mehr notwendig. Die Transformation von Gütern und Diensten in Daten erzeugen zunehmende Anreize und aufgrund der Entatofflichung des Geldes können Zahlungen Stand heute anonymisiert stattfinden. Die Folge ist eine wachsende Zahl von Cyberattacken auf Unternehmen und Behörden.

Daher ist es wichtiger denn je, die Entwicklungen der digitalen Transformation zu verstehen und zu vermitteln. Schulungen der Mitarbeiter können helfen, diese für die Gefahren von Ransomware zu sensibilisieren und den kritischen Umgang mit Hard- und Software zu verbessern.

Eine Entwicklung von der physischen zur Erpressung über Datentransfer bietet aber auch gewisse Vorteile. Die Opfer von Angriffen müssen sich beispielsweise in der Regel nicht um ihre (körperliche) Gesundheit sorgen. Dass Güter sich jetzt in Daten „verstecken“, ermöglicht die Existenz von Backups. Daten sind somit nicht notwendigerweise einzigartig und lassen sich durch eine Kopie ersetzen. So verlieren Unternehmen zwar gegebenenfalls einen Teil des Arbeitsfortschritts, der in den Daten steckt, allerdings sind sie nicht gezwungen auf die Erpressung einzugehen.

Allgemein ist das Problem Ransomware jedoch eine fast schon spieltheoretische Frage von Anreizen versus Abschreckungen:

Solange es mit wenig Aufwand und ohne die realistische Aussicht auf negative Konsequenzen möglich ist, Ransomware-Angriffe durchzuführen, wird das Problem weiter bestehen und bis zu einer eventuellen „Sättigung“ des Marktes wohl auch weiterwachsen. Die zunehmende Regulierung von Kryptowährungen und das wachsende öffentliche Bewusstsein für die Thematik und der zunehmende Druck auf politische Entscheidungen, könnten jedoch dazu beitragen, die Spielseite der Verteidigung in Zukunft zu stärken. Zu viel Aufmerksamkeit ist nicht das, was Kriminelle wollen, daher führen Ransomware-Gruppen regelmäßig Scheinauflösungen durch, um wenig später mit neuem Namen und abgeänderter Software wieder aufs Spielfeld zu treten. Es bleibt abzuwarten, wie sich die Domäne der Ransomware weiterentwickelt; klar ist aber, dass sie eine logische Folge des bisherigen Verlaufs des Digitalisierungspfades ist.

Simon Kern und Jason Hottelet

Literatur:

(1) https://dictionary.cambridge.org/us/dictionary/english/asset
(2) Die Entstofflichung des Geldes – Blockchain und Bitcoin https://mikropolis.org/tutorial-digitale-transformation-verstehen/
(3) https://www.heise.de/news/Ransomware-Whitepaper-Immer-neue-psychologische-Tricks-der-Kriminellen-6224023.html
(4) https://www.golem.de/news/ransomware-landkreis-dreimonate-nach-it-angriff-weiter-im-notbetrieb-2201-162275.html
(5) https://www.heise.de/news/Hacker-Angriff-ueber-ITDienstleister-Kaseya-trifft-Hunderte-Unternehmen-6128388.html
(6) https://www.heise.de/news/Ransomware-Wachsende-Bedrohung-durch-Professionalisierung-6439718.html

Fragen:

Was versteht man unter Ransomeware undter der Metapher Ransomeware as a service?

Welche Felder sind für den Einsatz von Ransomeware besonders interessant?

Wie lassen sich die Gefahren von Ransomeware einhegen?

Vertiefungsangebote:

siehe dazu die Literaturhinweise

Thomas Fischermann
Kritische Infrastruktur: "Es sind nicht immer nur böse Russen"
https://www.zeit.de/digital/2022-03/kritische-infrastruktur-

hackerangriff-it-sicherheit-manuel-atug-interview/komplettansicht