MURDERBOARD

WIE ALLES BEGANN

TALES OF THE CRYPT-OH.
BUCH EINS

KLAUDIA »JINXX« ZOTZMANN-KOCH
RENÉ »LYNX« PFEIFFER

FEATURED BY
DEEPSEC

Coverdesign: Klaudia Zotzmann-Koch

Inhalt

PREQUEL

WO KRIMI, PRIVATSPHÄRE UND IT-SICHERHEIT ZUSAMMENKOMMEN

Es war ein warmer Sommertag als ich einen Anruf eines Bekannten bekam der mich für ein Datenschutz-Coaching bei einem seiner Kunden engagieren wollte. Neben Krimischreiben bin ich auch im Bereich Datenschutz tätig helfe Selbständigen und kleinen Unternehmen dabei ihre Webseiten und auch die internen Abläufe Datenschutz-konform aufzubauen. Vielleicht eine etwas merkwürdige Mischung: Krimi und Datenschutz. Aber eigentlich auch nicht wie sich beim näheren Hinschauen dann herausstellte und was sich im Laufe der kommenden vier Blogposts zeigen wird. Bei der Anfrage meines Bekannten ging es nämlich um einen konkreten Verdacht dass Informationen aus dem Unternehmen abfließen und von der Konkurrenz verwendet würden.

Ich bereitete eine längere Fragenliste vor die sich zum Teil aus meinen Erfahrungen im Datenschutz speiste zum anderen aus sieben Jahren Erfahrung als Projektmanagerin in der Webentwicklung. Die Fragenliste zeigte ich René der als freiberuflicher Pentester arbeitet. Vielleicht kennen ihn einige von Euch aus der Datenschutz Podcast Folge zu »Pentesting« oder auch einigen seiner Vorträge bei der PrivacyWeek. Es dauerte eine gute halbe Stunde dann bekam ich die Antwort: »Sieht vollständig aus«. Und ich dachte mir: Krimiautorin

und IT-Sec – gute Mischung für so einen Auftrag! Kriminalistisches Denken kann helfen Kriminelle zu überführen. Was würde ich angreifen wenn ich es auf eine kleine Firma oder auch eine Einzelperson abgesehen hätte?

Wenig später bekam ich eine weitere Nachricht: »Mach ein Murderboard! Ein klassisches wer – wen – wann – wo – warum.«

Ich dachte: Sag ich ja Krimiautorin und IT-Sec.

Und eine dritte Nachricht folgte: »Ich hab eine Idee! Lass uns gemeinsam eine Murderboard-Blogpost-Serie schreiben!«

Und da sind wir nun: Dort wo Krimi Privatsphäre und IT-Sicherheit zusammenkommen.

Wir sind übrigens René »Lynx« Pfeiffer IT-Security Experte und Veranstalter der jährlichen DeepSec-Konferenz die Fachmenschen im Bereich IT-Sicherheit zusammenbringt und ein erlesenes Workshop- und Vortragsprogramm bietet. Und ich Klaudia »jinxx« (oder »jinxx-proof«) Zotzmann-Koch Autorin Podcasterin Datenschutzexpertin und seit 2016 Mitorganisatorin der jährlichen PrivacyWeek.

Vielleicht fragt Ihr Euch warum wir uns ewig damit rumschlagen eine Blogpost-Serie zu schreiben. Die Antwort ist recht einfach: Wir wollen zeigen dass Onlinekriminalität viel häufiger einfacher und zugleich vielfältiger ist als man meinen möchte. Dazu kommen meine Erfahrungen aus vielen Workshops in Schulen Volkshochschulen selbstorganisierten Webinaren und mehr dass die Fragen die gestellt werden stets dieselben sind. In allen Altersstufen von 12 bis 92. Dazu die einhellige Meinung »ich bin ja viel zu uninteressant für die« ohne nähere Definition wer »die« überhaupt sind. Und natürlich das allgegenwärtige »ich habe ja nichts zu verbergen« das mehr wie »ich hab' keinen Bock mich mit dem Thema auseinanderzusetzen« zu lesen ist und auf eine Themenbeliebtheit vergleichbar mit Kalorienzählen oder Hodenkrebs deutet. Über allem schwebt ein blindes Vertrauen in Technologie eine Heilserwartung dass Technik all unsere Probleme lösen kann und wird wenn wir sie nur machen ließen. Gepaart mit naiver Arglosigkeit gegenüber Firmen und Institutionen aber auch gegenüber Behörden und dem Staat.

Wir wollen Euch zeigen was aktuell (Frühjahr 2021) tatsächlich geht und machbar ist wie schwierig oder einfach es ist und was für Interessen dahinter stehen. Und wir wollen einige kurzweilige Leseminuten bereiten. Das Thema ist ernst aber man kann es zumindest unterhaltsam erzählen.

KAPITEL 1

SPUREN

DER ZEITFAKTOR

Spuren sind die »Metadaten« einer Tat eines Vorgehens einer Kommunikation oder auch einer Anwesenheit bzw. eines Dagewesenseins. Spuren zeigen uns auf dass etwas passiert ist aber häufig auch wie etwas passiert ist. Spuren betrachtet man immer im Nachgang denn sie müssen ja erst da sein um betrachtet werden zu können. Wie groß der zeitliche Abstand zwischen dem Entstehen von Spuren und der Betrachtung ist kann sich stark unterscheiden. So haben Forscher:innen 2017 untersucht wie Ötzi eine Mumie aus dem Eis der Ötztaler Alpen vor etwa 5.300 Jahren zu Tode gekommen ist und so einen Mord mit leichter zeitlicher Verzögerung aufgeklärt[1].

Manche Spuren verschwinden aber auch. Nicht nur die bekannten Spuren im Sand die man gestern noch fand … Auch z. B. K.O.-Tropfen können bereits 24 Stunden nach Verabreichung nicht mehr im Blut des Opfers nachgewiesen werden.

Es gibt auch Spuren die nicht als »Störfaktoren« erkannt werden die sich ins Bild fügen und keinerlei Stirnrunzeln bei geübten Betrachtern hervorrufen. Ein klassisches »sieht nach einem Unfall aus«. Oder

der Tod betagter Personen der keinen überrascht aber Erb:innen erfreut.

Und dann gibt es die Spuren die Onlineverbrechen hinterlassen. »IP-Adressen« und »Logdaten« klingen vielleicht kryptischer als Fußspuren, Herzrhythmusstörungen oder »Richtung aus der der Pfeil kam« sind aber ebenso aufschlussreich.

Die Zeit ist nicht nur bei Verbrechen oder in der Physik allgegenwärtig. Computer sind auf Taktgeber angewiesen. Damit sind Uhren und der Blick darauf ein ständiger Begleiter in der digitalen Welt. So ziemlich alle Werkzeuge die zum Programmieren verwendet werden ermöglichen einen leichten Blick auf die aktuelle Zeit. Zeiten oder Zeitstempel wie es so schön heißt sind digital ein hervorragender Ariadnefaden. An diesem kann man sich immer orientieren.

EIN AN SICH HARMLOSER BEGINN

Leon ist Student und hat einen schmalen Geldbeutel. Sein Computer ist kaputt und er braucht dringend einen neuen. Also geht er zu einem Computerladen der auch wiederaufbereitete (»refurbished«) Geräte anbietet. Er entscheidet sich für einen aufbereiteten Laptop. Sein defektes Gerät gibt er als Ersatzteillager in Zahlung.

DATENTRÄGER

Früher oder später muss etwas dauerhaft gespeichert werden. Unter dauerhaft versteht die Informatik den sogenannten nichtflüchtigen Speicher der Bits und Bytes für eine gewisse Zeitspanne auch ohne Stromversorgung speichern kann. Die digitalen Tontafeln können verschiedene Formen annehmen. Angefangen hat das Speichern mit magnetischen Datenträgern wie Bändern Disketten und rotierende Metallscheiben. Begleitend kamen optische Datenträger hinzu (CD, DVD, BluRay). Moderne Medien verwenden Computerchips die sich kleine elektrische Ladungen merken also speichern. Der eigentliche Vorgang des Speichers hinterlässt Spuren in Form von Magnetfeldern

elektrischen Feldern oder Materialeigenschaften ganz abhängig von der Methode.

Die Spurensuche auf und an Datenträgern beschäftigt sich mit dem Zugriff auf gespeicherte Daten und deren Analyse. Die Kopie spielt eine zentrale Rolle da alle Untersuchungen an Kopien des Originals durchgeführt werden. Man möchte so unabsichtliche Veränderungen während der Analyse verhindern. Was genau auf welche Weise von welchem Medium ausgelesen werden kann hängt stark von der verwendeten Technologie ab. Spuren finden sich überall wenn man nicht gerade einen Schmelzofen zwecks Vertuschung zu Hand hat. Selbst zerbrochene CDs können auf den Bruchstücken Datenfragmente enthalten. Das klingt sehr nach Film und Fernsehen aber es geht gelegentlich nur um kleine Datenmengen wie Passwörter Logins Schlüssel oder Metadaten. Dafür können schon kleine Teile des Ganzen ausreichend sein.

NETZWERKE

Versendet man Daten über ein Netzwerk so werden diese in kleinere Teile geteilt und einzeln über viele Zwischenstationen transportiert. Man kann sich das wie eine Lieferung vorstellen die in einer Reihe von handlichen Paketen versendet wird. Diese Pakete können natürlich jeweils Spuren erzeugen. Einerseits könnten die einzelnen Stationen Kopien der Pakete anlegen. Außerdem gibt es noch den digitalen Absender und Empfänger. Welcher Punkt mit welchem anderen Punkt kommuniziert lässt sich ebenso aufzeichnen. Bei komplexeren Protokollen kommen noch weitere Daten hinzu. Ein Webserver kann aufschreiben welcher Endpunkt (= welches Endgerät) wann welche Daten abgerufen hat. Daraus lässt sich beispielsweise der Zweck der Übertragung ableiten.

Diese Spuren müssen nicht immer automatisch erhoben und gespeichert werden. Die für die Spuren notwendigen Daten entstehen allerdings immer ob sie dann auch gespeichert werden oder nicht.

DATEIEN UND NACHRICHTEN

Digital wie auch analog sind Informationen immer in definierten Portionen vorhanden. Die Aktenordner und Bücher entsprechen Dateien. Notizzettel Postkarten und Briefe entsprechen Messenger Nachrichten und E-Mails. Das alles kann beliebig angeordnet sein – sortiert chaotisch an einem Platz (sprich auf einem Gerät) verteilt auf mehrere Orte oder Personen. Das Sichten und richtige Verbinden dieser Fundstücke ist eine hohe Kunst und erfordert Erfahrung. Mit Glück tragen Dateien Zeitinformationen in oder an sich. E-Mails haben oft einen Verlauf mit zeitlichen und örtlichen Informationen in ihrem Inhalt sofern sie vollständig vorliegen (sprich mit Umschlag und darauf befindlichen Poststempeln).

EIN NÄCHSTER SCHRITT

Leons defekter Laptop wird derweil beim Händler auseinandergenommen. Ersatzteillager im Wortsinn. Das defekte Mainboard wird entsorgt die restlichen Teile wie Tastatur Bildschirm Festplatte Touchpad und mehr kommen in Kisten mit weiteren Tastaturen Bildschirmen Festplatten und Touchpads und warten auf eine neue Verwendung. Als Erstes kommt der Bildschirm aus Austauschteil in einem anderen Laptop zum Einsatz dann die Festplatte. Diese wird formatiert und das System wird neu installiert. Und damit ist das nächste Gerät bereit für die nächste Lebensdauer.

METADATEN

Metadaten sind strukturierte Daten die bestimmte Merkmale der eigentlichen Daten beschreiben. Sie geben den Kontext vor und helfen die sie beschreibenden Daten zu verstehen und zu verarbeiten. Metadaten alleine können sehr verräterisch sein. Man kann beispielsweise Beziehungen ableiten. Wer mit wem in Kontakt steht ist durchaus interessant. Oft beziehen sich Metadaten auf Kommunikation. Neben

den Kommunikationspartnern gibt es auch manchmal eine inhaltliche Beschreibung. Bei Ermittlungen gilt als Faustregel generell: Je Metadaten desto besser.

Aus dem Alltag kennen wir Metadaten. Telefonnummern die Gerätekennung von Mobiltelefonen oder E-Mail Adressen sind Beispiele. Sie enthalten meist keine persönlichen Informationen sie können aber Personen zugeordnet werden.

---

1. https://www.wissenschaft.de/geschichte-archaeologie/oetzi-es-war-heimtuecki scher-mord

KAPITEL 2

ERMITTLUNGEN

BRIEFE ALS FENSTER ZUR WELT

Wenn junge Menschen die Welt entdecken dann freuen sie sich oft über Post. Wer hat es denn nicht gern wenn andere an einen denken? Sobald die Liebesbriefe vom Schwarm die Metamorphose in herzlose Schreiben mit Fenster hinter sich gebracht haben erkennen wir: Geld regiert deren Inhalt genau wie in dieser Geschichte.

Leon hat eine Angewohnheit. Beim Gang vom Briefkasten zurück fühlt er gerne die Bedeutung des Inhalts von Briefen mit den Fingern. Im konkreten Fall ist es das Schreiben der Kreditkartenabrechnung. Und es ist auf mehrere gehaltvolle Millimeter angewachsen. Leon hofft auf eine Änderung der Geschäftsbedingungen. Nach dem Öffnen stellt sich allerdings heraus dass es leider eine Aufstellung von Zahlungen ist. Er kann sich kaum an die einzelnen Posten erinnern. Es sind einfach zu viele – und die meisten davon sind nicht von ihm! In der Zahlenkolonne sind verschiedene Beträge angetreten und marschierten im Gleichschritt zur Gesamtsumme. Weder die Posten noch die Firmen die er angeblich bezahlt hat sagen ihm etwas. Langsam kehrt der Verstand zurück. Leon durchsucht seine Geldbörse

aber alle Karten sind noch da. Dann greift er zum Telefon und lässt die Kreditkarte sperren.

Die nächsten Tage ist Leon ziemlich beschäftigt damit eine neue Kreditkarte zu beantragen und Zahlungen zu stornieren. Neben dem Studium und seinem Teilzeitjob frisst das verdammt viel Zeit und Nerven. Vor allem Letzteres. Überhaupt zwei Ressourcen die bei uns allen endlich sind und die in Leons Fall an anderer Stelle besser eingesetzt gewesen wären.

Was ist ihm passiert?

KONTEN UND KARTEN

Die Beantwortung dieser Frage beginnt bei der Verwendung der Kreditkarte. In der analogen Welt überlegt man wann man die Karte wo und zu welchem Zweck benutzt hat. Oft ist das überschaubar und an geographische Orte gebunden. Digital wird das schwieriger weil Online-Händler oft die Möglichkeit bieten Kreditkarten in Nutzer:innen-Konten zu hinterlegen. Dadurch ergibt sich automatisch eine Verknüpfung an die Zugangsdaten dieser Konten. Ist man eingeloggt kann man von dieser Plattform aus Zahlungen tätigen. Meist wird für Online-Accounts ein Login und ein Passwort verlangt. Unter Umständen wird eine E-Mail Adresse als Login verwendet. Im Unterschied zur physischen Kreditkarte muss man nun klären welches Online-Konto für eine Zahlung verantwortlich ist. Wurde das Online-Portal kompromittiert? War das Passwort zu schwach? Oder hat sich jemand Zugang zum E-Mail Konto verschafft?

In Leons Fall sind mehre Möglichkeiten denkbar. Betroffene Konten können Teil eines Datenlecks geworden sein. Mit Pech wissen die Portale die die Daten »verloren« haben noch nichts davon und können ihre User:innen nicht über den Vorfall informieren.

Eine weitere Möglichkeit ist eine Schadsoftware auf den Geräten die verwendet wurden. Findiger Schadcode schaut auf Systemen nach hinterlegten Konten dem Browser-Verlauf in Dokumenten und anderen brauchbaren Daten. Diese werden hinausgeschleust und in

den Kommandozentren der Angreifenden analysiert. In der Regel stecken hinter solchen Angriffen ganze Kampagnen die gut vorbereitet und organisiert durchgeführt werden.

SOCIAL MEDIA ALTER EGO

Social Media Postings bewegen die Welt – besonders wenn Ex-Präsidenten Kurznachrichten zwitscherten. Man kennt ja die eigenen Timelines. Manche suchen sich vertrauenswürdige Quellen folgen ihnen und haben auf diese Art menschliche Filter für Informationen geschaffen die den täglichen Faktenfluss steuern sollen. Vertrauen formt Netzwerke.

Das Handy klingelt. Leon hebt ab.

»Bist Du jetzt total bescheuert? Wieso postest Du so einen Blödsinn! Ich hoffe Du bist betrunken!« kommt es ihm ohne Begrüßung entgegen. Es folgen mehrere Minuten Verständnislosigkeit die nicht aufgeklärt werden können. Einfach aufgelegt. Nach dem dritten Anruf vervollständigt sich das Bild. Sein Twitter-Konto publizierte laut seinen Freunden Dinge die rassistisch und nicht jugendfrei waren. Er macht sich sofort auf die Suche nach der Ursache stellt aber gleich fest dass sein Login nicht mehr funktioniert.

Dieser Vorfall ist nicht fiktiv und ist schon sehr vielen Personen passiert. Die Vertrauensketten in sozialen Netzwerken sind lohnende Ziele speziell wenn eine Klarnamenpflicht noch zur öffentlichen Identifikation führt. Die Zugangsdaten zu den Konten werden meist durch Diebstahl kompromittiert. Schadsoftware sucht gerne nach aktiven Zugängen um Dritten den Zugang zu gewähren. Leons Beispiel ist noch ein harmloser Fall wenn auch sehr peinlich für ihn als Betroffenen. Es geht ja nicht nur um die öffentlichen Nachrichten sondern auch um die direkte Kommunikation (eben die sogenannten »direct messages« bei Twitter, auf Instagram, Mastodon oder artverwandte Botschaften). Woher soll Leon oder auch ich wissen ob jemand mitliest?

. . .

Viele Anbieter melden wenn der letzte Login nicht plausibel ist. Manche melden immer wann man sich mit welchem Gerät von wo (geografisch oder netzwerktechnisch) eingeloggt hat. Das hilft nur wenn man diese Informationen auch registriert und Unregelmäßigkeiten auffallen. Empfohlen wird die sogenannte Zwei-Faktor-Authentisierung (oder auch two factor authentication, 2FA). Bei dieser wird der Login von einem zweiten Kanal begleitet der einen Code zur Überprüfung liefert. Das kann eine klassische SMS sein. Es gibt aber auch Codegeneratoren die zeitgesteuert Zahlen liefern die sich alle Minute ändern. Die Generatoren werden mit einem Wert gestartet der im jeweiligen Online-Konto hinterlegt ist. Stiehlt jemand die Zugangsdaten so fehlt (hoffentlich) der zweite Faktor und die andere Person kann sich dennoch nicht einloggen obwohl sie Login und Passwort erbeuten konnte.

Leon hatte keine 2FA für seinen Twitter-Account. Bis zu diesem Tag hatte er gedacht das wäre nur was für Datenschutz-Fanatiker und Leute die etwas zu verbergen hätten.

SCHÄTZE DER NETZE

Meist dreht sich alles um Geld. In der digitalen Welt kommen jedoch noch andere Aspekte hinzu. Die Waren und geldwerte Güter sind hier etwas vielfältiger. Gültige Bankkonten Kreditkarten Zugänge zu E-Mail-Konten oder ähnlichen Ressourcen wie Social Media Präsenzen stellen indirekt Werte da die gestohlen und gehandelt werden. Das Bild auf solche Vorfälle verzerrt sich dabei. Wir als Menschen denken ja gerne »Wieso sind die hinter mir her?«. Oder auch »Ich bin doch viel zu uninteressant für die.« Darum geht es aber nicht immer. Man wird auch zum Ziel wenn man Ressourcen hat die interessant sind. Echte E-Mail-Absender sind natürlich beliebt weil sie die Glaubwürdigkeit der gefälschten E-Mail erhöhen. Selbst Zugänge zu Webseiten sind eine gefragte Ware weil die Kriminellen dort oder auf den Webservern hinter der Webseite Daten für ihre Aktionen ablegen können. Einem Bekannten ist es unlängst passiert dass sein Blog zum

Versenden einer Schadsoftware namens Emotet verwendet wurde. Die Datei mit dem Schadcode lag auf seinem Server und aus aller Welt wurde die Datei über Phishing-Mails abgerufen und bei den Menschen die den Link in der Mail geklickt hatten auf den Rechner geladen. Alles wegen eines nicht aktualisierten Plugins im WordPress mit dem er seinen Blog betreibt.

Die Automatisierung multipliziert die Wertschöpfung. So manche Betrugsmail dürfte schon für Amüsement oder Verwunderung geführt haben. Wenn aber bei Millionen von E-Mails nur Bruchteile eines Prozents auf die Masche hereinfallen dann sieht die Bilanz gar nicht schlecht aus. All die Downloads der Emotet-Datei sprechen dafür. Dasselbe gilt für die anderen Bereiche. Natürlich lassen sich gestohlene Kreditkarten sperren und Passwörter von Konten ändern. Dazu muss der Diebstahl allerdings erst einmal auffallen. In der digitalen Welt sind Daten nicht einfach »weg« oder »verschwunden« sondern werden kopiert d.h. man bemerkt den unzulässigen Zugriff nicht sofort. Es fällt frühestens dann auf wenn die kopierten Zugangsdaten aktiv verwendet werden. Und das kann eine unbekannte Anzahl anderer sein die die Daten von irgendwo her haben und sie nun verwenden.

»Follow the money« ist daher nach wie vor gültig. Cui bono? Das Konzept ist nur generell auf Werte ausgeweitet.

VIRTUELLE MOTIVE

Neben Geld und Rache gibt es noch weitere Beweggründe für digitalisierte Kriminelle. Ein Faktor der schwer zu akzeptieren ist sind schlicht und einfach Ressourcen. Damit ist auch Rechenleistung gemeint. Alles was Zugang zum Internet hat und Code ausführen kann ist ein gutes Ziel. Es wird noch interessanter wenn es schlecht gesichert oder kaum überwacht wird. Nahezu alles was sich »IoT« (»Internet of Things«, vernetzte Dinge wie Zahnbürsten, Kameras, Kaffeemaschinen, Heizungsthermostate oder Personenwaagen etc.) nennt fällt in diese Kategorie. Ein anderes gutes Beispiel ist ein alter

Computer (oder ein altes Smartphone). Es darf auch ein Server sein egal ob in der Cloud oder selbst betrieben. Alt ist dabei relativ. Es reicht schon dass er mit Software ohne aktuelle Sicherheitsupdates betrieben wird da kann das Blech selbst noch so neu sein (IoT). Das System hat Speicherplatz kann Programme ausführen und darf das Internet verwenden. Damit ist es interessant weil es als Sprungbrett für weitere Aktionen dienen kann.

Diese Vorgehensweise erlaubt es den Ursprung von Attacken zu verschleiern. Der Ursprung ist selten die direkte Quelle bei Vorfällen. Für Betroffene ist es natürlich kein Trost Beifang zu sein.

Für Ermittlungen ist es wichtig Beziehungen herzustellen. Ist ein Opfer das eigentliche Ziel Mittel zum Zweck oder eine absichtliche Täuschung? Gelegentlich werden auch absichtlich falsche Spuren gelegt um die Zuordnung der Täter:innen in eine bestimmte Richtung zu lenken.

ERMITTLUNGEN

Katharina Müller ist Beamtin bei der Polizei. Cybersecurity die Leute mit den flinken Internetanschlüssen und dem vorinstallierten Tor-Browser für die Ermittlungen im sogenannten Darknet. Seit einiger Zeit kommt ihr ein Name immer wieder unter: Leon Dragic. Noch ist sich Katharina nicht sicher ob er Opfer oder nicht doch eher Täter ist. Wobei schon eine Menge Chuzpe dabei wäre wenn er die ganzen Server von denen aus Malware ins Netz verbreitet wird auf seinen bürgerlichen Namen angemietet hätte. Andererseits wäre es auch nicht das erste Mal dass ein Typ glaubt unverwundbar oder unauffindbar zu sein. Aber bisher hat sie sie alle gekriegt. Bei manchen hat es nur länger gedauert. Und die Liste mit Notizen zu Leon wird langsam aber sicher länger.

DER ROTE FADEN

Ein roter Faden bei der Motivation sind die Vorteile. Welchen Nutzen bringt ein kompromittiertes System oder ein Konto? Das ist nicht dieselbe Frage wie »cui bono?«. Die Frage wem nützt ein Angriff wird vielmehr zur Verschleierung eingesetzt. Welchen Nutzen hat ein System an sich? Was kann es sehen sprich worauf hat es Zugriff? Im Falle von IoT-Geräten kann eine Kaffeemaschine möglicherweise eine Menge andere Geräte im selben Netzwerk sehen. Oder was an Daten über dieses Netzwerk geschickt wird. Sie sieht vielleicht auch Mobiltelefone die möglicherweise nicht im selben WLAN eingeloggt sind aber über die Bluetooth-Schnittstelle mit der Kaffeemaschine kommunizieren. Und je nachdem was die Marketingagentur die die App zur Kaffeemaschine gebaut hat noch alles für »Marketingzwecke« braucht sieht sie auch das Telefonbuch auf so einem Mobiltelefon die Fotos auf einer SD-Karte gespeicherte Daten anderer Apps und vielleicht noch die Daten aus den Sensoren des Geräts wie Beschleunigungs- oder Lagesensor.

Der Gedanke an Sichtbarkeit und Zugriffe führt unweigerlich zu Vertrauensketten die selbst ein Ziel darstellen. Freunde von Freunden sind immer interessant weil sie einander vertrauen. Diese Methode wird für E-Mail- oder auch SMS-Betrug in allen Formen und Farben benutzt. Plausible Absender waschen die Nachricht rein. Der Schaden ist nur schlimmer wenn Angreifer:innen vollen Zugriff auf andere Konten haben.

KAPITEL 3

SERIENHACKER: ORGANISIERTES VERBRECHEN

ODER AUCH »GRAND THEFT DATA«

MOTIVATIONEN DER »COSA DATA«

Erhebt man Daten zu einem wertvollen Gut wird es automatisch gehandelt gehortet gestohlen und gefälscht. Digitale Abläufe lassen sich sowohl legal als auch illegal nutzen genau wie die Wirtschaft in der analogen Welt. Es geht allerdings beim Thema Cybercrime um viel mehr als nur die Daten selbst. Konten mit bestimmten Berechtigungen stellen auch einen Wert dar weil sie als Multiplikator fungieren. Ein Beispiel ist ein einfaches E-Mail Konto mit hinterlegten Kontakten (Adressbuch oder auch die Kontaktdaten in den vorhandenen E-Mails). Damit kommen gleich mehrere Eigenschaften zusammen: Identität Vertrauen und ein Archiv von Nachrichten. Das Archiv kann man direkt nach wertvollen Daten durchsuchen. Die Identität kann man mit Hilfe des Vertrauens der Kontakte für Betrug verwenden um weitere Zugänge zu mehr Konten und Daten zu bekommen.

Die Motivation ist unterm Strich immer etwas wie ein Vorteil oder Gewinn. Daten die sich direkt verkaufen lassen haben einen unmittelbaren Nutzen.

Öfter werden Daten in mehreren Schritten besorgt.

METHODEN: ORGANISIERT UND ORDENTLICH

Die Organisation bei digitalem Verbrechen folgt analogen Vorbildern. Es gibt Dienstleister für alle Rollen und Stationen die notwendig sind. Man findet alles was man auch in einem gut aufgestellten Unternehmen finden würde. Es gibt Techniker:innen Marketing einen Helpdesk für die Opfer (im Falle von Erpressungssoftware – ja, tatsächlich!) Notare Händler Sicherheitsexpert:innen Bankenwesen und was man sonst noch in der Wirtschaft benötigt. Diese Struktur impliziert die Vorgehensweise und die Vorbereitung von Operationen. So etwas wie dramaturgisch aufbereitete Szenen wo binnen weniger Minuten hektischer Tastaturanschläge ganze IT Anlagen durchlöchert werden gibt es nur im Fernsehen oder in erdachten Büchern. Die Realität ist viel einfacher und vor allem sehr routiniert.

WERTSCHÖPFUNGSKETTE DER SCHATTENWIRTSCHAFT

Die Schattenwelt ist voller Dienstleister die ihre jeweilige Expertise anbieten. Damit ergibt sich ein getreues Abbild der legalen Wirtschaft. Die Möglichkeiten für Geschäfte ergeben sich aus den Kooperationen. Betrugskampagnen erheben über E-Mail-Aussendungen Daten von Opfern. Diese Daten werden zu Datenbanken zusammengefasst. Diese gehen an Raffinerien welche die Rohdaten durch Überprüfung und Klassifizierung veredeln. Man muss übrigens nicht einmal einen Link in einer E-Mail klicken damit die eigene E-Mail-Adresse dem Konvolut einverleibt wird. E-Mails enthalten häufig »Tracking-Pixel« und es reicht die E-Mail zu öffnen (oder in der Vorschau anzusehen) um das Tracking zu triggern und an den Absender zu melden dass diese E-Mail geöffnet wurde. Allein durch das Ansehen der E-Mail bestätigt man also dass es eine echte und aktive E-Mail-Adresse ist die weiterverkauft werden kann. Damit steigert sich der Wert der einzelnen Datensätze. Die so aufbereitete Ware geht dann an Händler weiter die auf Marktplätzen die Produkte anbieten. Dort findet man neben den Handelstreibenden auch Käufer Notare und Bezahldienst-

leister (bis hin zu Banken und Geldwäschern) die für eine sichere Abwicklung der Transaktionen sorgen. Eine Krähe hackt der anderen vielleicht kein Auge aus aber man geht doch lieber auf Nummer sicher. Immerhin kennt man sich wahrscheinlich nicht.

DIE ÜBLICHEN VERDÄCHTIGEN

Oder man kennt sich vielleicht doch. Die üblichen Verdächtigen eben. So wie die 30 bis 80 Leute auf der Beobachtungsliste von Katharina Müller. Sie surft tagaus tagein auf den üblichen Seiten hat die Angebote im Blick genauso die Anbietenden. Nicknames ändern sich immer wieder es kommen auch ständig Leute dazu oder fallen raus. Aber der »harte Kern« ist immer da unter irgendwelchen Namen. Für weite Teile ihres Jobs muss sie nicht einmal den Tor-Browser starten das meiste passiert im ganz normalen Internet. Zwischen den Neuzugängen ist seit letztem Monat ein oder eine »ldra002«. Scheint recht aktiv zu sein. Sie schreibt den Namen auf ihre Liste.

KAPITEL 4

TROJANISCHER AMTSSCHIMMEL

ODER AUCH: STAATLICHES HACKEN

TAUBENFÜTTERN IM PARK – SPIONAGE

Wissen ist Macht. Nichts wissen macht neidisch wenn man das Modell moderner Informationsgesellschaften ansieht. Die natürliche Anwendung von Netzwerken die Informationen transportieren ist Spionage. Das Internet hat daher schon früh Bekanntschaft damit gemacht. Der Aspekt Nachrichten in einen Bereich hinein und hinaus zu schleusen ist offensichtlich. Damit verbunden ist auch das Durchbrechen von Sicherheitsmaßnahmen um Zugang zu geschützten Informationen zu kommen.

Wobei weite Teile unserer eigenen Informationen viel weniger geschützt sind als es uns lieb oder auch nur bewusst wäre. Die vorher genannten E-Mails werden grundsätzlich im Klartext und für alle einsehbar verschickt. Eine unbekannte Anzahl Dritter liest sie auf dem Weg von Absender:in zu Empfänger:innen mit und wertet diese Informationen aus. Und alle Informationen die wir in Accounts auf US-amerikanischen Plattformen haben (Fotos, mehr oder weniger öffentliche Postings, Direktnachrichten etc.) sind für Behörden in den USA und allen die mit den USA kooperieren einsehbar. Es wäre nicht das

erste Mal dass Menschen wegen eines Social Media Postings oder eine Direktnachricht auf einer Plattform nicht in ein Land einreisen dürfen.

BEFEHLSKETTE

Martin B. aus A. verdient sein Geld als Auftragnehmer. Er hat eine kleine Firma unter der er gute alte EDV-Dienstleistungen anbietet: Drucker einrichten die Netzwerke kleiner Unternehmen warten ab und an mal eine Webseite für Einzelunterehmer:innen bauen. Das macht den Kohl nicht fett aber es bietet einen validen Überbau für sein eigentliches Geschäft. Martin B. kümmert sich um ein paar Command- & Control-Server die von mehreren großen Kampagnen im Netz verwendet werden um Schadsoftware zu kontrollieren und zu steuern. Er weiß nicht wie seine Auftraggeber heißen. Die letzten drei hatten lange Zeichenketten als Nickname angegeben. Sein Geld bekommt er von wechselnden Nummernkonten in unterschiedlichen Cryptowährungen. Meist existieren diese Konten nur wenige Tage. Er hat es aufgegeben ihnen nachzugehen. Er will es auch gar nicht wissen. Martin B. verwendet in unregelmäßigen Abständen selbst immer wieder andere Nicknames und andere Nummernkonten. Eins für jeden Zahlungseingang. Nur sehr selten verwendet er Nickname und Nummernkonto zweimal. Momentan ist er als »ldra002« unterwegs. Und sein Auftrag ist einen neuen Command- & Control-Server für eine Schadsoftware namens Ryuk hochzufahren. Die ihm genannten Spezifikationen sind beeindruckend groß und gibt gutes Geld. Vermutlich haben seine Auftraggeber damit etwas Größeres vor. Martin B. fragt nicht nach. Nachfragen ist schlecht fürs Geschäft. Stattdessen zieht er zufällig eine der unlängst frisch eingekauften Kreditkarten aus dem digitalen Dateikasten und mietet einen virtuellen Server für 21 Tage bei einem großen Anbieter. Er schmunzelt als er den Namen liest: Leon Dragic. Wie lustig und sehr passend zu seinem aktuellen Pseudonym. Schon übermorgen wird er ein anderes verwenden – weit bevor dieser Leon die Rechnung bekommt.

EXPLOSIVE APPS – SABOTAGE

Bei ausreichender Digitalisierung kann man sowohl die Produktion von Waren als auch die Zerstörung von Produktionsstätten den Maschinen überlassen. Wo man früher noch mühsam Sprengstoff schmuggeln und durch Agenten anbringen lassen musste so kann man das heute durch Software erledigen lassen. Industrieanlagen wie Stromversorgung Energietransport in Form von Pipelines chemische oder nukleare Verarbeitungsprozesse Fertigungen oder verwandte Konstrukte reagieren durchaus anfällig auf Ausfälle. Man kann auch in Mess- und Steuerungsabläufe eingreifen um Maschinen gewollte Entscheidungen auf Basis falscher Werte abzuringen. Diese Art der digitalen Sabotage äußert sich selten durch spektakuläre Explosionen. Es reicht völlig wenn eine Produktion zum Erliegen kommt oder Serienfehler aufweist. Die beste Sabotage wird lange nicht bemerkt.

Für die Ausführung solch perfider Angriffe kann man eigene Leute beauftragen oder für viel Steuergelder schweigsame Dienstleister:innen engagieren.

Ein Themenbereich der an dieser Stelle vielleicht angeschnitten werden sollte ist der sogenannte »Staatstrojaner«: ein Stück Software das viele Probleme mit sich bringt. Angefangen damit dass wir mittlerweile in einer Gesellschaft leben in der die Regierenden allen Bürger:innen ein grundsätzliches Misstrauen entgegenbringen und wir alle unter Generalverdacht stehen den nächsten Terroranschlag zu planen. Daher gibt es eine Spionagesoftware die allen Bürger:innen untergeschoben werden können soll.

Schon allein der Weg dahin dass diese Software überhaupt existiert ist gepflastert mit allerlei Problemen. Beispielsweise dass man für eine Schadsoftware eine Möglichkeit finden muss dass diese überhaupt Zugriff auf passende Daten bekommt. Im Fall von ungesicherten oder nur minimal gesicherten Geräten wie IoT-Geräten ist dies einfach. Aber unsere Mobiltelefone auf die Regierungen abzielen weil sie unsere persönliche Kommunikationszentrale darstellen sind schon eine

ganz andere Nummer und normalerweise recht gut abgesichert. Um dort »Root-Rechte« (Super-Admin, quasi »Gott«) zu erhalten muss man schon eine richtig dicke (und damit teure) Sicherheitslücke finden. Und die gibt es sogar. Nicht umsonst bringen die Hersteller unserer Geräte alle Nase lang Sicherheitsupdates heraus um immer wieder frisch gefundene Lücken zu schließen und die Betriebssysteme und Apps sicher zu halten. So gut es eben geht. Es gibt allerdings auch hier einen großen Schwarzmarkt auf dem gefundene Sicherheitslücken meistbietend verkauft werden. Wenn Ihr bis hierher mitgelesen habt wird Euch das nicht weiter verwundern. Kriminelle finden immer wieder Wege um Geräte zu kompromittieren. Im Gegensatz zu Sicherheitsforschern die im Grunde dasselbe tun ihre Erkenntnisse allerdings den Herstellern melden und ihnen helfen die Lücken zu schließen und die Welt für alle Menschen ein bisschen sicherer zu machen schlagen die Kriminellen daraus Geld. Und: cui bono? Wer kauft diese Lücken ein? Andere Kriminelle und Regierungen die damit Staatstrojaner gegen ihre eigenen Bürger:innen bauen. Für viel Steuergeld wird ein hochproblematischer Schwarzmarkt nicht nur am Leben erhalten sondern regelrecht befeuert.

Auch in der Anwendung sind solche Spionageprogramme problematisch. Zum einen rechtlich da eine Schadsoftware zur Kommunikationsüberwachung sehr tiefe Rechte auf einem Mobiltelefon braucht. Wenn sie z.B. Kommunikationsdaten in sicheren Messengern mitlesen können soll muss sie die Inhalte vor dem Verschlüsseln auf dem Gerät der Absender:in mitlesen können. Ein sicherer Messenger sendet die Daten »Ende-zu-Ende-verschlüsselt« also ist der Inhalt der Nachricht ausschließlich an den beiden Enden bei Absender:in und Empfänger:in lesbar. Auf dem Weg dazwischen sieht man zwar dass eine Nachricht existiert der Inhalt ist allerdings von außen nicht lesbar sondern nur »Zeichensalat«. Eine Schadsoftware die nun Nachrichteninhalte vor dem Verschlüsseln mitlesen und nach außen weiterleiten können soll braucht Super-Admin-Rechte auf dem Mobiltelefon. Und damit kann sie alles lesen was auf dem Gerät passiert inklusive Telefonbuch Fotos

Inhalte anderer Apps Telefongespräche mithören und was das Gerät eben alles kann. Das ist viel viel mehr als Behörden eigentlich dürften aber weniger geht technisch gar nicht damit die Schadsoftware ihren Dienst tut.

Und last not least das Problem wo Anwendung und Einkauf der Sicherheitslücken zusammenfallen: Die Beweisbarkeit. Wer sagt dass Kriminelle diese eine Sicherheitslücke (oder auch die vielen) nur an diese eine Regierung verkauft haben? Es kann jede:r auf einem Schwarzmarkt alles kaufen wenn das nötige Kleingeld da ist. Und drei- vier- oder auch fünfstellige Summen können sich auch Privatpersonen oder hoch professionell aufgestellte Kriminelle wie wir sie oben schon geschildert haben durchaus leisten. Wenn nun jede:r eine entsprechende Schadsoftware erstellen kann wird es schwer zu argumentieren dass bestimmte Beweise wirklich von einer bestimmten Person sind. Wir erinnern uns an die Admin-Rechte: Jede:r kann durch entsprechende Schadsoftware und damit verbundene Zugriffsrechte auf Mobilgeräte Fotos GPS-Verläufe und mehr fälschen und so sind Beweise plötzlich keine Beweise mehr. Sondern höchstens die Frage wer welche Geschichte erzählen will was mit diesem Gerät alles gemacht wurde wo es dabei war was es gesehen oder gehört haben soll.

Aber weil wir jetzt schon soviel Steuergeld für solche Software ausgegeben haben müssen wir sie auch einsetzen sonst wäre ja alles umsonst gewesen. Was man hat muss man auch nutzen. Erstaunlicherweise planen aber 80 Millionen Deutsche und auch 8 Millionen Österreicher:innen gar keine Terroranschläge. Sie sind auch nicht in Kinderschänderringen organisiert. Die meisten wissen nicht einmal wo sie im Netz nach Bauanleitungen für hochexplosive Dinge oder zu Recht verbotenen Fotografien suchen sollten und haben auch noch nie vom Tor-Browser für einen Zugang zum sogenannten Darknet gehört. Um genau zu sein sind die meisten auch froh mit dem ganzen Zeug nichts zu tun zu haben und leben einfach ihr normales Leben. Was also tun mit dieser atomaren Erstschlagswaffe? Ein paar Spatzen

finden sich zumindest bei Erpressung Drogen- und Eigentumsdelikten[1]. Und andere europäische Länder finden ihre eigene Bevölkerung auch nicht so knorke wenn diese sich für Unabhängigkeit vom Zentralstaat ausspricht[2].

Am Ende bleibt dabei über dass für einen staatlich geplanten Einsatzzweck gegen einige wenige Kriminelle die Mobilgeräte für alle Menschen unsicher gehalten werden. Weltweit. Für Steuergeld. Und damit Tür und Tor offenstehen durch die Kriminelle mit allen Geräten anstellen können was ihnen beliebt.

DIE FÜNFTE DIMENSION – KRIEG UND PROPAGANDA

Zuerst führte man Krieg auf dem Land. Dann kam das Wasser dazu. Die Luft ist als Kriegsschauplatz noch jung. Noch jünger ist der Weltraum. In diesen Reigen gesellt sich seit wenigen Jahrzehnten das Internet. Die Welt des digitalen Krieges oder auch »Cyber Warfare« genannt nennen die Militärs die fünfte Dimension. Gekämpft wird mit Software die entweder Angriffe abwehrt oder auch durchführt. Man verbindet Elemente der Informationssicherheit (oder -unsicherheit) mit den Vorgaben militärischer Missionen. Spionage und Sabotage ist dabei inbegriffen.

Die Informationshoheit wird bei diesem Thema oft vergessen. Die Manipulation von Informationen ist ebenso ein Teil des Ganzen. Eine Beeinflussung von Nachrichten politischen Entscheidungen Wahlen oder Meinungen in der Öffentlichkeit kann gravierende Folgen haben. Die Sprache wird dabei zur Waffe und das Internet ist das Trägersystem. Fatal an dieser Art der Manipulation ist dass selbst eine temporäre Darstellung von Botschaften schon eine Wirkung haben kann.

STAATLICHES HACKEN BEI ERMITTLUNGEN

Wo ermittelt wird da fallen manchmal digitale Späne. Das trifft auch auf den digitalen Teil der Nachforschungen zu. Leider trifft dort die

Forensik auf die Informationssicherheit. Grundaufgabe der Informationssicherheit ist das Verhindern von Angriffen dem Abgreifen von Daten und der Kompromittierung von Systemen. Organisiertes Verbrechen oder die Angriffe von Nationen halten sich aber nicht an Gesetze. Oft diskutiert wird daher in diesem Zusammenhang das sogenannte »hack back« oder »Zurückhacken« bei Angriffen. Dabei wird aktiv auf einen Angriff ein Gegenangriff auf die echten oder vermeintlichen Täter:innen ausgeführt. Die Kontroverse dabei ist ob man tatsächlich die Richtigen erwischt oder nur Passanten bzw. ahnungslose Stellvertreter:innen die zufällig an der Attacke beteiligt sind. Ein weiterer Punkt ist der Verlust der Vertrauenswürdigkeit von Online-Plattformen und digitaler Infrastruktur wenn Hintertüren zum Zugriff auf Daten und digitalen Aktivitäten eingeführt werden. Hauptargument für die Hintertüren ist der Schutz von Daten durch Verschlüsselung. Sicherheitsgurte mit Sollbruchstellen sind aber keine mehr. Besagte Hintertüren können von Ermittler:innen und Verbrecher:innen gleich benutzt werden. Verlierer:innen sind wir dabei alle.

IMPLIKATIONEN UND KONSEQUENZEN FÜR DIE INFORMATIONSSICHERHEIT

Aufgabe der Informationssicherheit ist der Schutz digitaler Daten und Infrastrukturen. Die dazu notwendigen Hilfsmittel sind Barrieren die die digitalen Güter vor unbefugtem Zugriff schützen. Darunter fällt die sichere Verschlüsselung der Schutz des Transports und des Aufbewahrungsorts sowie beschränkter Zugriff auf Daten und Systeme. Die Qualität des Schutzes hängt von den zur Verfügung stehenden Mitteln ab. Zugriff auf IT Systeme oder Daten durch Dritte kann nur mit einer Hintertür oder den dafür vorgesehenen Zugangsberechtigungen. Möchte man sich vor Zugriff durch Dritte schützen so bleiben für Ermittler:innen und Angreifer:innen nur Schwachstellen oder Nachschlüssel. Damit ist dann die Umsetzung von Informationssicherheit nicht mehr möglich. Die Technologie wertet die Zugriffe nicht ethisch.

Ein Zugriff durch Dritte bleib ein Ein- oder Angriff. Der Kontext entscheidet. IT Spezialist:innen können bei Anzeichen von Zugriffen kaum den Kontext feststellen bevor Daten kopiert werden. Rein technisch gibt es auch keinen guten oder bösen Zugriff. Der Zugriff auf Daten bleibt wertneutral. Jegliche Schwächung der Sicherheitsmaßnahmen schwächen die Fähigkeiten der Verteidiger:innen.

DAS KLICKEN DER HANDSCHELLEN

Katharina Müller ist in Jubelstimmung. Sie und ihre Kolleg:innen haben gerade einen ganz großen Fisch an Land gezogen. Einer der Hintermänner einer groß angelegten Schadsoftware-Kampagne gegen das Innenministerium sitzt nebenan im Verhörzimmer. Zu ihrer eigenen Verblüffung ist er geständig. Besonders interessant ist mit wem er es sonst noch so zu tun hatte und wer mit in der Sache drinsteckt.

Katharina geht ihre Notizen noch einmal akribisch durch. Ein Name taucht auch hier immer wieder auf. Zur selben Zeit am selben Ort … Leon Dragic. Die GPS-Daten seines Telefons sprechen Bände. Vier von sieben Malen war er im selben Café einmal auf einer Demo vor der Tür. Sie ist sich mittlerweile sicher dass Leon einer dieser Typen ist die sich ihrer selbst zu sicher sind. Sie hat ihn auf Fotos von zwei Demonstrationen gefunden. Reißt darauf ganz schön das Maul auf.

Katharina schickt den Haftbefehl an die Kolleg:innen die Leon herbringen werden.

Wir hoffen wir konnten deutlich machen dass es einen ganz zentralen Aspekt bei Onlineverbrechen gibt: Vertrauen. Vertrauen ist ein seit Langem gelerntes Verhalten gegenüber anderen Menschen – seit den Mammuts. Mit all der Technologie die heute um uns und zwischen uns ist liegt das Vertrauen – leider – viel zu oft an der falschen Stelle.

. . .

Ende. (Vorerst.)

---

1. https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/
2. https://www.golem.de/news/nso-group-spanien-setzt-offenbar-staatstrojaner-gegen-katalanen-ein-2007-149659.html

QUELLEN

https://www.wissenschaft.de/geschichte-archaeologie/oetzi-es-war-heimtueckischer-mord

https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/

https://www.golem.de/news/nso-group-spanien-setzt-offenbar-staatstrojaner-gegen-katalanen-ein-2007-149659.html

Links zur Blog-Serie »Murderboard« auf Englisch:

https://blog.deepsec.net/murder-board-blog-series-prequel/

https://blog.deepsec.net/murder-board-blog-series-chapter-1-traces/

https://blog.deepsec.net/murder-blog-series-chapter-2-investigations/

https://blog.deepsec.net/murder-board-blog-series-chapter-3-serial-hackers-organized-crime-or-grand-theft-data/

https://blog.deepsec.net/murder-board-blog-series-chapter-4-trojan-horses-or-state-hacking/

Links zur Blog-Serie »Murderboard« auf Deutsch:

https://www.zotzmann-koch.com/murderboard-prequel-wo-krimi-privatsphaere-und-it-sicherheit-zusammenkommen/

https://www.zotzmann-koch.com/murderboard-kapitel-01-spuren/

https://www.zotzmann-koch.com/murderboard-kapitel-02-ermittlungen/

https://www.zotzmann-koch.com/murderboard-kapitel-03-serienhacker-organisiertes-verbrechen-oder-auch-grand-theft-data/

https://www.zotzmann-koch.com/murderboard-kapitel-04-trojanischer-amtsschimmel-oder-auch-staatliches-hacken/

DeepSec Blog: https://blog.deepsec.net/

Murderboard-Talk von René und Klaudia bei der PrivacyWeek 2020 #pw20:

https://media.ccc.de/v/pw20-367-murderboard-wo-krimi-privatsphre-und-it-sicher heit-zusammenkommen

Über die Autor:innen

René »Lynx« Pfeiffer IT-Security Experte und Veranstalter der jährlichen DeepSec-Konferenz die Fachmenschen im Bereich IT-Sicherheit zusammenbringt und ein erlesenes Workshop- und Vortragsprogramm bietet.

Mastodon: https://chaos.social/@nightlynx

Klaudia »jinxx« (oder »jinxxproof«) Zotzmann-Koch ist Autorin Podcasterin Datenschutzexpertin und von 2016 bis 2021 Mitorganisatorin der jährlichen PrivacyWeek.

Mastodon: https://literatur.social/@viennawriter

Murderboard ist *Featured by DeepSec*.

Weitere Awareness Kurzgeschichten gibt es auf:

https://www.zotzmann-koch.com/stories/

Erstellt mit Vellum