LAYER 8

Ihre Schnittstelle zwischen IT und Recht.

LAYER 8 GmbH
Zentralstrasse 20
Postfach 1343
CH-6031 Ebikon/Luzern

+41 41 511 5008
contact[at]layer-8.law
https://layer-8.law

Forensic Readiness Massnahmen (Teil 2)

Vorbereitung auf forensische Untersuchungen – organisatorische und technische Massnahmen

> *"Forensic Readiness" has two objectives:*
>
> 1. *Maximizing an environment's ability to collect credible digital evidence, and;*
> 2. *Minimizing the cost of forensics in an incident response.*
>
> *John Tan, Forensic Readiness, 2001*

Rechtsanwalt Roman Kost, MLaw, CAS Informationssicherheit

Digitale Forensik bezweckt die rechtsgenügliche Gewinnung von Beweisen; Forensic Readiness bedeutet, diese Beweisgewinnung auch praktisch durchführen zu können. Im ersten Teil (Forensic Readiness - Teil I) wurden die Grundlagen dargestellt (Strafprozessordnung, ISO 27037:2012 und ISO 27043:2015-Standards, zentrale Prinzipien der digitalen Forensik, SAP-Modell. In diesem zweiten Teil des Beitrags werden nun Massnahmen aufgezeigt, um ein angemessenes Niveau der Beweissicherungsfähigkeiten zu erreichen (sog. Forensic Readiness), wobei es gleichzeitig die eingesetzten Ressourcen effektiv zu nutzen und die Kosten zu minimieren gilt. Dafür wird auf die wesentlichen organisatorischen und technischen Massnahmen eingegangen. Anhand von fünf praktischen Fällen wird abschliessend die Relevanz von Forensic Readiness im heutigen Wirtschaftsleben aufgezeigt.

Digital Forensics, Forensic Readiness, Informationssicherheit, Strafprozess, Zivilprozess

[v. 2023-02-02]

Inhaltsverzeichnis

1. Abstract

[1] Digitale Forensik bezweckt die rechtsgenügliche Gewinnung von Beweisen.

[2] Im ersten Teil (Forensic Readiness - Massnahmen) wurden Grundlagen dargestellt: Es wurde auf die Bedeutung der Schweizer Strafprozessordnung im Bereich des Beweisrechts für Zivilverfahren erläutert. Sodann wurde auf die Standards ISO 27037:2012 und ISO 27043:2015 eingegangen und die zentralen Prinzipien der digitalen Forensik (Akzeptanz des Vorgehens, Wahrung der Integrität, Dokumentation) sowie das SAP-Modell (Secure – Analye – Present) aufgezeigt. In diesem zweiten Teil des Beitrags werden nun Massnahmen dargestellt, um Forensic Readiness zu erreichen:

[3] Um die digital-forensische Beweisgewinnung zu unterstützen, werden im Rahmen der Forensic Readiness-Massnahmen organisatorischer und technischer Natur ergriffen. Mit Forensic Readiness will eine Organisationseinheit systematisch ein angemessenes Niveau ihrer Beweissicherungsfähigkeiten erreichen und dabei gleichzeitig die eingesetzten Ressourcen effektiv nutzen und die Kosten minimieren. Das eigentliche Sichern von digitalen Beweisen wird dagegen mit Begriff Digital Forensic erfasst.

[4] Zu den wesentlichen organisatorischen Massnahmen zählen das Implementieren von Forensik-Prozessen auf Basis von Forensik-Strategien und/oder risikospezifischen Policies. Eng an forensische Prozesse gekoppelt sind Business Continuity bzw. Business und Desaster Recovery-Strategien.

[5] Die technischen Massnahmen unterliegen einem stetigen Wandel, weshalb konkrete Produktvorschläge nicht sinnvoll sind. Zur grundlegenden Funktionalität der technischen Massnahmen gehört aber in jedem Fall das Dokumentieren von Vorgängen, was häufig durch die Implementation von Netzwerk und/oder Host Based Intrusion Detection Systemen erfolgt, mit denen eine Vielzahl von Daten und Metadaten erfasst werden.

[6] Anhand von fünf Fällen aus dem Wirtschaftsleben wird am Schluss aufgezeigt, dass Forensic Readiness grosse Bedeutung hat und auf dem Radar moderner Unternehmen auftauchen muss.

2. Erreichen einer adäquaten Forensic Readiness

[7] Im Rahmen der Vorbereitungshandlungen stellt sich die Frage, welche Ressourcen man für den Ernstfall bereitgestellt haben will.

[8] Die Implementation von Forensic Readiness kann dabei dem Standard ISO 27043:2015, dem Standard für die Untersuchung von Vorfällen folgen sowie ISO 27037:2012, dem Standard für digital-forensische Untersuchungen. Auf beide Standards wurde schon im ersten Teil des Beitrags verschiedentlich hingewiesen.

[9] Speziell erwähnt werden muss das Buch von JASON SACHOWSKI, Implementing Digital Forensic Readiness - From Reactive to Proactive Process, 2. Aufl., Florida 2019. Es dürfte soweit ersichtlich die erste umfassende Abhandlung zum Thema Implementation von Digital Forensic Readiness sein. SACHOWSKI wirft dabei zahlreiche zentralen Fragen im Hinblick auf organisatorische und technische Massnahmen auf, die ein Unternehmen treffen sollte. Dazu bietet er diverse Handreichungen in Checklistenform an.

[10] In den nachfolgenden Absätzen folgt ein grober Überblick, der die notwendigsten Ansätze anschneidet, um die Forensic Readiness einer Organisationseinheit auf ein angemessenes Niveau zu heben:

a. Organisatorische Massnahmen ergreifen

i. Ist-Zustand der IT-Landschaft erfassen

[11] Zur Implementierung eines angemessenen Niveaus von Forensic Readiness muss man als allererstes die aktuelle Lage kennen. In Unternehmen sind Bestandesaufnahmen von Prozessen und unterstützender IT nach einem ausgewählten Regelwerk die Praxis (z.B. COBITv5, ISO 27001, ITIL). Alle haben gemeinsam, dass der Prozesseigner und damit auch dessen Vorgesetzte bis hin in die Chef-Etage auf den letzten bekannten Stand zugreifen können, wenn Bedarf besteht.

ii. Mögliche Risiken eruieren / Risiken kennen

[12] Nachdem die aktuelle IT-Umwelt bekannt ist, müssen mögliche Risikoszenarien eruiert werden. Auf Basis der selbst benutzten Technologie kann die Organisation ableiten, wo der nächste Schadenfall eintreten wird. Zumindest muss sie es versuchen. Zu den Standardrisiken gehören heute z.B. eine Verschlüsselung durch einen Erpressungstrojaner, Missbrauch der IT durch Mitarbeiter etc. Grundrisiken dieser Art sollten in jedem Fall Eingang in die Überlegungen haben.

[13] Beim Eruieren die Sicht des Angreifers einzunehmen und sich z.B. zu fragen "Welches Ziel lohnt sich bei uns?", kann wertvolle Inputs liefern. Ebenso zu wissen, was man von aussen als wertvoll erraten oder vermuten könnte (Fragen Sie jemanden ausserhalb der Organisation!), beim Ausfall welcher Komponenten die Arbeit nicht mehr möglich ist, welche Kanäle werden täglich oder gar ständig benutzt und ebenso was sich weniger als Angriffsziel lohnt, kann die Einschätzungen qualitativ verbessern.

[14] Zur Risikokenntnis gehört auch, dass die verantwortliche Person (CISO oder ein Chef Sicherheit oder ähnliches) das aktuelle Tagesgeschehen im Securitybereich beobachtet. Es sollten Newsletter bei den verschiedenen Meldestellen erfasst werden.[1] Weiter gehört dazu, sich mittels einschlägiger Medien auf dem Laufenden zu halten.[2]

[15] Die verantwortliche Person sollte dafür von ihren 5x8 oder 9 h Arbeitszeit mindestens eine halbe Stunde verwenden dürfen. Besser noch: müssen. Aktuelles Wissen ist absolut zentral, um bei Vorfällen nicht völlig im Dunklen zu tappen. Häufig genügt es schon schlicht "einmal davon gehört zu haben". Dann nämlich kann man sich das Wissen gezielt und in kurzer Zeit erschliessen, wenn es notwendig wird. Es gilt das Motto: Know your Enemy.

iii. Mögliche Strategien definieren

[16] Es ist nicht möglich, alle potentiellen Szenarien abzudecken. Alleine schon die endlichen Ressourcen, die man zugeteilt bekommen hat, setzen einem umfassenden Vorhaben ein Ende. Auch die eigenen Fähigkeiten und Kenntnisse, mögen sie auch noch so gross sein, wirken limitierend. Alles kann man nicht wissen.

[17] Häufig genügt es, eine solide Grundstrategie zu entwickeln. Diese Grundstrategie enthält Anweisungen, die für jeden Mitarbeiter verständlich sind (einfache und untechnische Sprache). Jeder Mitarbeiter im

[1] Z.B. MELANI-Newsletter, Newsletter BSI, CVE-Newsletter

[2] Man lese z.B. heise.de resp. deren Security-Channel, golem.de etc. pp.

Unternehmen, dem ein Incident auffällt, soll sich daran orientieren können.

[18] In einer Grundstrategie sind im Minimum Benachrichtigungsketten enthalten und klare Definitionen, wer für was zuständig ist und wer wen ersetzt, sollte jemand ausfallen. Das ist nichts anderes als die Einrichtung eines CSIRT (Computer Security Incident Response Team). Einem Gesichtspunkt muss man besonderes Augenmerk schenken: Wer beurteilt einen möglichen Vorfall als relevanten Vorfall? Wichtig ist dabei, dass mehrere Personen involviert sind. Dadurch reduziert sich u.a. das Problem eines Angreifers, der selber im CSIRT sitzt. Ebenso wird die Qualität der Beurteilung durch das Mehraugenprinzip besser und es entsteht eine gewisse Ausfallsicherheit, sollte die beurteilende Person entfallen.

[19] In die Grundstrategie gehören auch Überlegungen zur Kommunikation und Öffentlichkeitsarbeit oder der Beizug von spezialisierten Anwälten. Zum Beizug von spezialisierten Anwälten muss namentlich für die Kommunikation mit einer gegnerischen Partei, der Polizei oder den Staatsanwaltschaften dringend geraten werden. In die Kontakteliste gehört auch das MELANI. Der Bund stellt mit dieser Dienststelle wertvolles Knowhow zur Verfügung. Es kann auch notwendig sein, das eine oder andere CERT im Vorfeld kontaktiert zu haben, damit man im Ernstfall darauf zurückgreifen kann.

[20] Diese ganz grundsätzliche Strategie gehört in eine Issue Specific Policy (neben z.B. Policies für Cybercrime-Fälle, Policy für den Brandfall etc.). Die Forensic Readiness Strategie sollte sich auch in der übergeordneten Information Security Policy widerspiegeln.

[21] Es kann auch sinnvoll sein, eine eigenständige Forensic Strategy aufzustellen.[3] Das Management hält darin fest, wie sie das gewünschte Mass an Forensic Readiness erreichen will. Darauf aufbauend wird eine Forensic Policy definiert, mit welcher u.a. festgehalten wird, wie das Personal bei einem Vorfall zu reagieren hat, wie das CSIRT (vorstehend [18]) vorzugehen hat und welche Infrastruktur zwecks Forensic Readiness betrieben werden soll.

[22] Man kann darüber streiten, ob die Definition von Policies und Strategien nicht an erster Stelle stehen soll, also noch vor dem Verschaffen des Überblicks. Argumente für oder gegen einen spezifischen Ausgangspunkt gibt es an sich keine, die wirklich stichhaltig wären. Schliesslich hat man diesen Schritt zu irgendeinem Zeitpunkt in Angriff zu nehmen. Wenn es erst im Rahmen der Bewältigung eines Zwischenfalls dazu kommt, ist das zwar bedauerlich, aber nicht mehr umkehrbar. Wichtig ist, *dass* man es macht.

[23] Ganz eng an die Strategien der Incident Response geknüpft sind Business Continuity resp. Disaster Recovery-Pläne.[4] Es ist zwar gut, dass man auf einen Vorfall reagiert und ihn digital-forensisch untersuchen kann, die Geschäftsprozesse müssen aber trotzdem aufrecht erhalten bleiben. Würde man sich bei einem Vorfall mit einem Verschlüsselungstrojaner nur mit der Beweissicherung beschäftigen, kann das dem Unternehmen das Genick brechen, womit dann auch die ganze Beweissicherung keinen Nutzen mehr hat. Wen will man noch in Verhandlungen oder einem Prozess damit unterstützen?

[24] Mit Business Continuity werden die negativen Auswirkungen des Vorfalls abgeschwächt oder gar ganz behoben; bei der Desaster Recovery will man sich

[3] ISO 27043:2015, S. VII oben.

[4] SACHOWSKI, S. 47.

möglichst rasch von der eingetretenen Katastrophe erholen und wieder produktiv werden. Die digitale Forensik dagegen ist ein nebenherlaufender Prozess parallel dazu. Die Kunst ist es, das Zusammenspiel dieser beiden Prozesse so auszugestalten, dass sie sich nicht allzu stark gegenseitig hemmen oder sich gar gegenseitig die Zielvorgaben zunichtemachen. Ist der Fokus vollständig auf Business Continuity, besteht die Gefahr, dass die Grundlagen für die digitale Forensik vernichtet werden: Ersetzt man den betroffenen Server oder setzt man ihn neu auf? Beim Neuaufsetzen gäbe es für die Forensik nicht mehr viel zu sichern. Auch das kann durchaus eine Strategie sein: Man akzeptiert das Risiko von Schadenfällen, forciert die Wiederaufnahme eines produktiven Betriebs und verzichtet auf Forensik.

[25] Zusätzlich zur Grundstrategie ist es sinnvoll, für eruierte Spezialfälle zugeschnittene Abläufe zu definieren. Zu denken ist an Missbrauch der IT-Anlagen durch Mitarbeiter (Filesharing, Pornokonsum (legaler oder illegaler Art), Spionage, etc.).[5]

b. Technische Massnahmen ergreifen

[26] Hier stellt sich ganz allgemein die Frage, welche Tools man einsetzen will. Dabei ergeben sich zwei unterschiedliche Betrachtungsweisen: 1. Welche Tools werden gebraucht, um einen konkreten Vorfall zu untersuchen und aufzubereiten? 2. Welche Tools werden eingesetzt, um stetig Beweissicherung vorzunehmen und Vorfälle zu detektieren, quasi als Begleitprozess zu den Betriebsabläufen?

i. Für die Untersuchung eines konkreten Vorfalls

[27] Wie schon dargelegt, haben Produktvorschläge immer ein Ablaufdatum; sie sind wenig sinnvoll. Eine Ausnahme zu dieser Regel findet man mit einem Blick in den RFC 3227 - Guidelines for Evidence Collection and Archiving aus dem Jahr 2002. Die Autoren listen unter dem Titel *'Tools you'll need'*[6] verschiedene altgediente Programme auf: 'ps' für die Auflistung der laufenden Prozesse, 'ifconfig', 'netstat' und 'arp' für das Auflisten Netzwerkzustände oder 'dd' für bitweises Kopieren. Diese Veteranen trifft man auch heute noch auf nahezu jedem Unix-like Betriebssystem an. Analyse-Software und -Frameworks bauen dann häufig auf ebendiesen Tools auf und bieten eine benutzerfreundliche Oberfläche und Reportingfunktionen an.

[28] Für eine forensische Untersuchung sollten Systeme genutzt werden, die nicht Teil des zu untersuchenden Systems waren. Entweder werden z.B. frische Laptops benutzt und die notwendigen Anwendungen installiert oder man hält entsprechende Geräte dauerhaft bereit. SACHOWSKI hält fest, dass alle Tools ihre Eigenheiten haben und unterschiedlich arbeiten. Der Forensiker muss diese Unterschiede kennen.[7]

[29] Damit das Thema Forensikprodukte nicht vollständig ausgeklammert wird, folgendes: Hinweise zu geeigneten Tools finden sich bei DOLLE, S. 185 und eine gute Hilfestellung zur Evaluation der Tools kann dem Anhang C: "Tool and Equipment Validation Program" bei SACHOWSKI entnommen werden.

---

[5] SACHOWSKI, S. 53 ff. spricht dabei vom Definieren von Business Risk Scenarios. Das schlägt auch ISO 27043:2015, S. 9 vor.

[6] Die genannten Tools (bis auf dd) nutzt man aber nur im Bereich der Liveanalysen, also dort, wo man ein laufendes System antrifft und den laufenden Zustand untersuchen will. Liveanalysen sind stark problembehaftet, da auf Datenträger gespeicherte Informationen verändert werden können. Vom Inhalt des Arbeitsspeichers (z.B. des RAM) gar nicht erst gesprochen. Abgesehen davon kann Malware das Starten von Prozessen überwachen und sich gezielt selber löschen oder gar das System zerstören. Jede Liveanalyse wird sich zudem der Schwierigkeit ausgesetzt sehen, wie sie dokumentiert werden soll.

[7] SACHOWSKI, Appendix C: Tool and Equipment Validation Program oben.

ii. Für die stetige, begleitende Beweissicherung

[30] Als ständig begleitender Prozess ermöglicht Forensic Readiness eine laufende Beweissicherung. Die Beweissicherung erfolgt ohne konkreten Anlass. Als ständiger Prozess können damit später auch Ereignisse nachgewiesen werden, die eine grosse Latenzzeit haben. Angriffe z.B. auf die RUAG wurden erst Jahre nach dem initialen Angriff aufgedeckt. Im Fall der RUAG hat man bezeichnenderweise erst ab dem Jahr 2014 verdächtige Kommunikationsmuster nachweisen können und geht heute davon aus, dass die Täterschaft bereits ein oder zwei Jahre zuvor Zugriff auf das Netz erhielt. Alles was vor 2014 passierte, wurde nicht aufgezeichnet (siehe zum Hackerangriff auf die RUAG Rz [45]).

[31] Anspruchsvoll ist die Frage, welche technische Mittel man überhaupt zum Einsatz bringen will. Die Fülle an Produkten ist überwältigend und es ist nicht immer gesichert, dass die Produkte am Ende das einhalten, was sie versprechen. Es kann sich als sinnvoll erweisen, auf Open Source Produkte zu setzen: Diese Produkte findet man nicht allzu selten unter der Haube von teuer verkaufter Software mit.[8] Das Management muss hier Rückgriff auf Fachleute nehmen. Die Angriffsszenarien genau gleich wie die Angriffsvektoren unterliegen ständigem Wandel, hier muss die Technik immer à-jour sein.

[32] Ebenso anspruchsvoll ist die Frage, wo die gewählten technischen Mittel in der IT-Infrastruktur platziert werden. Um diese Frage beantworten zu können, muss man die Funktionsweise der Technik gut kennen, die man einsetzen will. Was kann sie, was nicht? Detektiert man damit auf gewünschte Weise einen Incident? Wie läuft das Reporting dieses Incidents ab, wie und wie rasch wird reagiert? Wie und wie lange werden die gewonnen Daten gespeichert?[9]

[33] Die Beweissammlung kann passiv sein, indem z.B. Datenverkehr mitgeschnitten wird oder auch aktiv geliefert werden, wobei z.B. Tools auf einem Client laufen und relevante Datensätze an eine zentrale Sammelstelle gesandt werden. Die Rede ist dabei von NIDS (Network Intrusion Detection Systems) und HIDS (Host-based Intrusion Detection Systems). Liefert ein HIDS urplötzlich keine Daten mehr, obwohl es sollte, löst auch das auf der Empfängerseite einen Alarm aus. Kombiniert man beide Funktionsarten, so spricht man von Hybriden IDS.[10]

[34] Die Archivierung der gesammelten Beweise kann zu einem Problem werden. Um an das einleitende Beispiel der RUAG (Rz [30] resp. [45]) anzuknüpfen: Bei der Grösse eines Netzes, wie es die RUAG (mutmasslich) betreibt, fallen enorme Mengen an Daten an. Wenn die Täterschaft während eines Angriffs mehrere GB an interessanten Datensätzen erbeutet, liegt es auf der Hand, dass zugehörige Metadaten rasch selber ein Vielfaches davon aufweisen. Von den nicht einschlägigen Datensätzen gar nicht erst gesprochen. Kurz: Beim Implementieren von Forensic Readiness muss der Archivierung des gesammelten Materials das notwendige Augenmerk geschenkt werden.

---

[8] Zu nennen sind Produkte wie Security Onion (https://securityonion.net), SNORT (https://www.snort.org) oder Suricata (https://suricata-ids.org).

[9] ISO 27043:2015 folgt einem risikobasierten Ansatz, in dem Business Risk Scenarios eruiert werden. Die Frage nach dem "was" wird als Beweis gesichert, behandelt SACHOWSKI, Kap. 8, ausführlich. Er unterteilt grob in Background Evidence und Foreground Evidence. Ersteres kann man als Grundrauschen bezeichnen (Logfiles auf den Servern, Routern, IPS/IDS etc.), zweiteres als gezielt gesammeltes Beweismaterial, um einer Täterschaft ein Tun nachzuweisen.

[10] Zur Übersicht: https://de.wikipedia.org/wiki/Intrusion_Detection_System (letztmals abgerufen am 18.11.2019)

[35] Ganz abgesehen vom Umfang, welche die gesammelten Daten über die Zeit erhalten, muss zu jedem Zeitpunkt sichergestellt werden, dass diese Daten nicht verändert werden können. Ohne die Integrität sicherzustellen, haben die gesammelten Daten keinen Beweiswert (vgl. Grundprinzip Integrität, Rz 32 des ersten Teils des Beitrags).

3. Fünf Praxisfälle zur Forensic Readiness

i. Emotet-Angriff auf das Unternehmen O.

[36] Das Unternehmen O. musste im Jahr 2019 eine massive Störung des Betriebs hinnehmen.[11] Die Schadsoftware-Kombination Emotet-Trickbot-Ryuk schlug zu und verschlüsselte sämtliche Fileserver wie auch Datenbanken und Systeme, die für Mailkommunikation eingesetzt wurden. Es wurde eine Forderung von 45 Bitcoin gestellt. Gemäss dem CEO war das Unternehmen faktisch tot.

[37] Die Vorgesetzten beim Unternehmen O. konnten innert weniger Tage (und glücklicherweise über ein Wochenende) die grundlegende Betriebsfähigkeit und – was bei einem Büromaterialvertrieb besonders wichtig war – die Kommunikation mit den Kunden wiederherstellen. Auf der Webseite wurde auf die Störung hingewiesen, alle Kunden angerufen und mitgeteilt, man solle weiter bestellen, es laufe wieder. Die Kunden hatten gutgemeint damit begonnen, das Unternehmen O. zu schonen und vorderhand auf Bestellungen verzichtet. Wäre dieses Schonen durchgeschlagen, hätte das zusätzliche negative Konsequenzen auf die Betriebsresultate gehabt. Den Ausfall von Bestellungen über eine Woche oder länger hinweg, hätte enorme Nachwirkungen mit sich gebracht.

[38] Das Unternehmen O. hat u.a. die bestehende Hardware ausgesondert, neue Laptops angeschafft, neue Mailadressen erstellt[12] und eine Vielzahl weitere Massnahmen getroffen, die im Verlaufe der Business Recovery notwendig wurden.[13]

[39] Das Unternehmen O. war nicht auf diesen Emotet-Trickbot-Ryku-Angriff vorbereitet. Es gab keine Forensic Readiness und keine festgelegte Incidence Response. Über die anschliessende forensische Untersuchung und prozessuale Behandlung bei den Untersuchungsbehörden ist aus öffentlichen Quellen noch nichts zu entnehmen. Die Firma InfoGuard sowie das MELANI (der Vorgängerorganisation des NCSC) haben aber gewisse Kommunikationslinien zu den Command & Control-Servern beobachtet. Das könnte ein Startpunkt für die Strafverfolger sein, doch ist im Zusammenhang mit Computerdelikten und der zähen internationalen Rechtshilfe bei dieser Ausganslage (keine Forensic Readiness mit stets mitlaufender Beweissammlung) eher von geringem Erfolg auszugehen. Die Täter dürften straflos davonkommen.

[40] Ganz ohne Vorbereitungen war das Unternehmen O. aber nicht. Die Vorbereitungen waren zwar nicht formell existent, sondern direkt in den Personen

[11] Diese Informationen stammen aus dem öffentlichen Vortrag von 27.08.2019 anlässlich des 27. August - Schweizer Tag der sicheren Digitalisierung (organisiert von Prof. Dr. B. Hämmerli) und basieren auf Gedächtnisnotizen. 100% Richtigkeit ist nicht garantiert. Beispielhaft seien diese Berichte noch angefügt: Die NZZ hat ebenfalls darüber berichtet: https://www.nzz.ch/wirtschaft/cyber-angriff-auf-schweizer-firma-offix-ein-kampf-ums-ueberleben-ld.1492862 sowie Halbjahresbericht 2019/1 des MELANI, S. 8 und 11.

[12] Bei den Mails wurde festgestellt, dass der benutzte Provider Google Spamschutz betreibt. Beim Anschreiben aller Kunden hat man Blockaden festgestellt, die bei Massenversänden über 50 Mails zu greifen begonnen, und musste mehrere Accounts erstellen.

[13] https://www.inside-it.ch/articles/54898 (letztmals abgerufen am 21.11.2019).

der Vorgesetzten angelegt. Die Vorgesetzten waren in Krisenmanagement und Führung geschult und konnten so ad hoc Lösungen generieren und am Ende das Steuer herumreissen.

[41] In so einer Situation sind Stress und Fehler nicht vermeidbar, können aber mit entsprechenden organisatorischen Massnahmen (Grundstrategien, evtl. risikospezifische Strategien, Forensic Readiness) massiv reduziert und der ganze Prozess erheblich effizienter ausgeführt werden.

ii. Phishing Angriff auf hosttech.ch

[42] Der Hoster hosttech wurde am 28.08.2019 für eine Phishing-Welle missbraucht. Es wurden E-Mails im Namen und im Kleid von hosttech versendet, mit dem Ziel, Kundendaten abzugreifen. Hosttech gibt an, rund 1.5h nach dem ersten Erkennen der Phishingmails zu reagieren begonnen und zwar als allererstes eine Meldung ans MELANI vorgenommen zu haben. Im Anschluss sei der Hoster der Betrugsseite angeschrieben, Google Safe Browsing und Consorten orientiert und durch einen geschickten "Trick" den Betrügern ein Bild untergeschoben zu haben, das auf die Betrugsmasche hinweist. Die Betrüger haben ein Bild ab dem Hosttech-Server gesourced, was hosttech nutzte und es durch ein Bild mit den Lettern "FAKE" ersetzte. Auf der Betrügerwebseite wurde dann dieses trojanisierte Bild den Opfern angezeigt.[14]

[43] Man erkennt: hosttech hat ein Monitoring auf Phishing-Attacken, bei denen ihr Label missbraucht wird. Vermutlich handelt es sich beim Monitoring-Instrument um einen sensibilisierten Mitarbeiter, der dann entsprechend reagiert. Es bestehen Prozesse, wie auf diese Vorkommnisse reagiert wird, wozu die Meldung an staatliche Stellen wie auch die Kommunikation mit den Kunden und sogar der Öffentlichkeit (Öffentlicher Bericht im Internet) abgedeckt werden. Zugleich wird überwacht, ob sich Kunden von unüblicher Seite her einloggen, also womöglich die Angreifer die Zugangsdaten der Opfer ausprobieren. Solche Konten werden gesperrt und die Inhaber orientiert.

[44] Ob hosttech im Anschluss auf die Phishingwellen die Untersuchungsbehörden eingeschalten hat, ist nicht öffentlich bekannt. Steht der Betrügerserver in einem europäischen Land, wären die Chancen intakt, dass die Strafverfolger die Täter ermitteln können.

iii. (Wirtschafts-)Spionage: Angriff auf die RUAG

[45] Die RUAG stellte im Vorfeld des 21.01.2016 fest, dass sich nichtautorisierte Personen seit langer Zeit (mutmasslich mehrere Jahre, gesichert seit Sept. 2014) in den internen Netzen lateral bewegten. Es kam in der nachweisbaren Zeit zu einem Datenabfluss von geschätzten 23 GB. Bis zur Aufdeckung des Angriffs vergingen 1,5 Jahre (Kommissionsbericht, S. 3 unten). Die bisher geschaffene Transparenz durch technische Analyserapporte der GovCERT/MELANI ist bemerkenswert und fehlt beim Bundestagshack nach 2016 vollständig.[15]

[14] Sämtliche Informationen von https://www.host-tech.ch/blog/phishing-attacke-hosttech (letztmals besucht am 18.11.2019).

[15] Zum ganzen Vorfall: Bericht GPK-NR vom 08.05.2018 "Standortbestimmung: Bewältigung des Cyber-Angriffs auf die RUAG": https://www.parlament.ch/centers/documents/de/bericht-gpk-n-cyberangriff-ruag-2018-05-08-d.pdf; Sowie der Bericht des MELANI vom 23.05.2019: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/fachberichte/technical-report_apt_case_ruag.html (letztmals besucht am 19.11.2019).

[46] Die Täter exfiltrierten Daten im Mäntelchen von http-Traffic und Benutzten POST-Requests zu zuvor gehackten unauffälligen Webservern, womit u.U. Deep Packet Inspection / IPS / DLP-System unterwandert werden konnten. Es wurden auf den Servern Scripts verwendet, die sich als Google Analytics-Scripts tarnten; ebenso wurden URL-Shortener eingesetzt. Dem Angriff lag bekannte Schadsoftware (Turla, figuriert auch unter dem Namen Ouroboros[16]) zu Grunde.

[47] Die Täter hielten ihr Profil durch striktes Beachten einer Ziele-Liste (Angriff nur gegen Geräte, die auf der Liste enthalten waren) klein, was für einen ressourcenstarken Angreifer spricht. Der Initialvektor des Angriffs konnte nicht mehr sicher eruiert werden, da die Logfiles vor 2014 nicht mehr existent (ob solche überhaupt existiert hatten, ist nicht bekannt). Die benutzte Reconnaissance-Software hat Payload nachgeladen, um sich die Persistenz in den RUAG-Systemen zu sichern; im Anschluss wurden Daten ausgeleitet. Eher unkonventionell war das Aufspannen eines P2P-Netzes zwischen Bots im RUAG-Netz zur Kommunikation untereinander und das Benutzen von Kommunikationsdrohnen zu externen, zuvor bereits übernommenen Webservern. Damit wurde auch das Kommunikationsprofil kleingehalten.

[48] Das Beispiel der RUAG zeigt, wie mächtig Beweissicherungsprozesse sein können. Das Vorgehen der Täterschaft konnte detailliert nachvollzogen werden. Gleichzeitig erkennt man eindrücklich, dass über die Phase vor 2014 nichts bekannt ist. Vor 2014 existierten keine Aufzeichnungen.

iv. Zweckwidrige Internetnutzung während der Arbeit: Pornokonsum

[49] Auch das übermässige Vermischen von privaten Angelegenheiten mit der beruflichen Tätigkeit ist ein Thema für Forensic Readiness und die anschliessende digitale Forensik. Der Hintergrund sind hier eher arbeitsrechtliche Pflichten, sowie strafrechtliche Tatbestände (siehe dazu das Fallbeispiel ab Rz [54] nachfolgend), die Mitarbeiter mit IT-Infrastruktur einer Organisationseinheit setzen.

[50] Der Konsum von Pornografie am Arbeitsplatz ist in aller Regel arbeitsrechtlich untersagt. Regelungen finden sich in Arbeitsverträgen oder zusätzlichen Vereinbarungen, die der Arbeitnehmer unterzeichnet. Sie ergeben sich aber auch aus dem Treueverhältnis zwischen Arbeitnehmer und Arbeitgeber. Ist die Vertrauensgrundlage derart schwer verletzt, dass eine weitere Beschäftigung der betreffenden Person nicht mehr zuzumuten ist, darf gar fristlos gekündigt werden (Art. 337 Abs. 1 OR).

[51] So geschehen im Falle zweier SBB-Mitarbeiter, denen man stundenlagen Konsum von Pornografie nachweisen konnte. Das Monitoring erfolgte durch die SBB-IT-Abteilung, der aufgefallen war, dass langandauernde Verbindungen zwischen einschlägigen Webseiten und den Benutzerclient bestanden hatten. Die fristlose Kündigung wurde durch das Bundesverwaltungsgericht geschützt.[17] Ebenso letztinstanzlich vom Bundesgericht. [18] Diese zweckwidrige Verwendung des Internets währen der Arbeitszeit führte zu einem nicht

[16] Siehe https://de.wikipedia.org/wiki/Turla (letztmals besucht am 02.02.2023).

[17] Medienmitteilung des Bundesverwaltungsgerichts vom 18.12.2015: https://www.bvger.ch/dam/bvger/de/dokumente/2015/12/a-5641_2014_a-64532014zweiangestelltedersbbwegenzweckwidriger-int.pdf.download.pdf (letztmals besucht am 02.02.2023).

[18] Urteil 8C_79/2016 des Bundesgerichts vom 30.06.2017 (italienisch) abrufbar unter:

weiter zumutbaren Vertrauensbruch, der eine fristlose Entlassung rechtfertigte.

[52] Das Beispiel dieser beiden SBB-Mitarbeiter zeigt auf, dass Forensic Readiness auch dazu dienen kann, die eigenen Ressourcen zu kontrollieren. Mitarbeiter sollen während der entlohnten Zeit ihre Arbeitskraft in den Dienst des Arbeitgebers stellen und nicht Pornografie konsumieren. Bei 4h täglichem Pornografiekonsum, wie es den beiden SBB-Mitarbeitern nachgewiesen werden konnte, sind 50% der Arbeitskraft vernichtet und im gleichen Masse Lohn ohne Gegenwert ausbezahlt worden. Dank der gezielten Überwachung konnte dieser Missstand behoben werden.

[53] Es stellen sich bei der Überwachung der Internettätigkeit der Arbeitnehmer zahlreiche komplexe Fragen aus den Bereichen Datenschutz und Arbeitsrecht. Wer eine solche Überwachung durchführen will oder im Sinne von Forensic Readiness ein ständiges Beweissammeln implementieren will, sollte den rechtlichen Kontext genau abklären. Bei solchen Überwachungsmassnahmen sind ausserdem die strafrechtlichen Grenzen im Auge zu behalten.[19]

v. Zweckwidrige Internetnutzung während der Arbeit: Stalking

[54] Mit den ständig wachsenden Kommunikationsmöglichkeiten, der damit zusammenhängenden Anonymität und der erstaunlichen Sorglosigkeit mit privaten Angaben im Internet, häufen sich Stalkingfälle, bei denen das Internet benutzt wird.[20]

[55] Stalker weisen sehr häufig psychische Auffälligkeiten auf. Ihr Tun stellt entweder nur vorübergehend ein von der Norm abweichendes Verhalten dar oder hat effektiv andauernden Krankheitswert. Stalkern ist nicht zwingend bewusst, was ihr Tun bei der gestalkten Person auslöst. Die Distanz des Internets trägt seinen Teil dazu bei. Dass Stalker aber die Grenzen des Strafrechts mit ihrem Tun überschreiten, wenn das Stalking ein grösseres Ausmass erreicht, ist ihnen meistens bewusst.

[56] In den Schweizer Gesetzen findet sich nirgends eine Legaldefinition von Stalking. Das Zivil- und das Strafrecht erfassen aber typische Erscheinungsformen von Stalking und bieten Abwehrmittel. Das Strafgesetzbuch erfasst den Missbrauch von Telekommunikationsmitteln mit Art. 179^{septies} [21] StGB, wobei x-faches Telefonieren wie auch massenhaftes E-Mail-zuschicken erfasst sind. Sollte sich das Opfer solcher Tätigkeiten in seiner Handlungsfreiheit beschränkt fühlen, so wird der Tatbestand der Nötigung nach Art. 181 StGB eröffnet sein. Wer jemanden belagert (sei es nun auf der Strasse oder auf Facebook) und diese Person dazu zwingt, nicht mehr den gleichen Weg oder die gleiche

http://www.polyreg.ch/bgeunpub/Jahr_2016/Entscheide_8C_2016/8C.79__2016.html (letztmals besucht am 02.02.2023).

[19] Mit diesen Ausführungen muss es sein Bewenden haben. Ein interessantes Papier zu diesem Thema hat das Staatssekretariat für Wirtschaft SECO publiziert: https://www.seco.admin.ch/dam/seco/de/dokumente/Arbeit/Arbeitsbedingungen/Arbeitsgesetz%20und%20Verordnungen/Wegleitungen/Wegleitungen%203/ArGV3_art26.pdf.download.pdf/ArGV3_art26_de.pdf (letztmals abgerufen am 02.02.2023).

[20] Die Schweizerische Kriminalprävention hat sich diesem Thema mit einer Webseite angenommen: https://www.skppsc.ch/de/themen/gewalt/stalking/ (letztmals eingesehen am 02.02.2023).

[21] Das Gesetz spricht von "Fernmeldeanlagen", worunter von Telefon bis Computer – also auch E-Mail-Kommunikation – alles erfasst wird.

Kommunikationsplattform zu benutzen, der nötigt das Opfer und wird vom Strafrecht erfasst.[22]

[57] Benutzt nun eine angestellte Person betriebliche Infrastruktur, namentlich den Firmencomputer oder das Firmennetz zum Stalken, begeht er mit dieser Infrastruktur Delikte. Erhält der Arbeitgeber Kenntnis davon, z.B. durch eine Meldung des Opfers, wird er sich fragen müssen, ob er solches Verhalten tolerieren will. Branchen wie die Versicherungswirtschaft, Banken oder Pflege reagieren sensibler als andere Branchen.

[58] Wird mit der Firmeninfrastruktur ein Mitarbeiter durch einen anderen gestalkt, hat der Arbeitgeber sogar eine Handlungspflicht. Er ist arbeitsrechtlich verpflichtet, die Gesundheit seiner Arbeitnehmer zu schützen (Art. 328 OR). Dieser Pflicht kann er nachkommen, indem er dem Stalker das Fehlverhalten nachweist und ihn mit den entsprechenden Mitteln massregelt oder ihn bei den Untersuchungsbehörden anzeigt.

[59] Für den Nachweis des Fehlverhaltens kann der Arbeitgeber wiederum auf die Forensic Readiness zurückgreifen und deren Resultat beiziehen. Es stellen sich hier dieselben Problemfelder, wie bei jeder Überwachung von Arbeitnehmern (siehe vorstehend [53]).

4. Abschliessende Gedanken zu den Massnahmen im Rahmen von Forensic Readiness (Teil II)

[60] In Anbetracht der nicht zu unterschätzenden Kosten, die Forensic Readiness und insbesondere die darauffolgende prozessuale Auseinandersetzung mit sich bringt, stellt sich die Frage, wie kleine Unternehmen sich diesem Thema stellen sollen.

[61] Einfach auf solide Backupstrategie setzen und keine Gedanken daran zu verlieren, wer nun wie den Vorfall verursacht hat, kann durchaus eine valable Alternative zu einer vollumfänglichen und kostenintensiven Forensic Readiness-Strategie sein.

[62] Ein Mittelding erscheint auf den ersten Blick weniger sinnvoll: Hat man zwar den Beweis, wer den Schadenfall in welcher Art und Weise verursacht hat, verzichtet danach aber darauf, mit voller Konsequenz die Angelegenheit vorprozessual oder prozessual zu verfolgen, muss man sich die Frage nach dem Sinn der eingesetzten Mittel fragen. Noch weniger Sinn hätte das Sammeln von unverwertbaren Beweisen.

[63] Wichtig ist ebenfalls, nicht zu stark auf technische Mittel zu setzen. Die Arbeit verrichtet auch in absehbarer Zukunft noch der Mensch; Technik soll ihn dabei unterstützen. Schwieriger zu implementieren – aber auch umso wirkungsvoller – ist eine gut aufgestellte Organisation.

[64] Es kommt dazu: Beweise werden weiterhin von Menschen bewertet, weshalb sie auch von Menschen verstanden werden müssen. Das Gleiche gilt für technische Lösungen. Das Abstellen auf intransparente und sehr oft geradezu magisch anmutende KI, um nur ein Beispiel zu nennen, genügt der aktuellen Rechtslage in keinem Fall. Zumindest im Moment noch.

[22] Es gäbe noch diverse weitere Facetten von Cyberstalking. Einige davon lassen sich hier nachlesen: https://www.skppsc.ch/de/themen/gewalt/stalking/ (letztmals abgerufen am 02.02.2023) im Kapitel "Recht" sowie hier: https://de.wikipedia.org/wiki/Stalking (letztmals abgerufen am 02.02.2023).

Literaturverzeichnis

SACHOWSKI JASON	*Implementing Digital Forensic Readiness - From Reactive to Proactive Process*, 2. Aufl., Florida 2019
TAN JOHN	*Forensic Readiness*, Cambridge, 2001 elektronisch abrufbar unter: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.480.6094&rep=rep1&type=pdf

Materialienverzeichnis

Bericht GPK-NK	Standortbestimmung: Bewältigung des Cyber-Angriffs auf die RUAG, GPK-NK, vom 08.05.2019 https://www.parlament.ch/centers/documents/de/bericht-gpk-n-cyberangriff-ruag-2018-05-08-d.pdf letztmals abgerufen am 02.02.2023
Bericht MELANI RUAG	Technical Report about the Malware used in the Cyberespionage against RUAG, MELANI, vom 23.05.2016 https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/dokumentation/fachberichte/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf letztmals abgerufen am 02.02.2023
Bundesverwaltungsgericht zu SBB-Mitarbeiern	*Zwei Angestellte der SBB wegen zweckwidriger Internetnutzung entlassen*, Bundesverwaltungsgericht, vom 18.12.2015 https://www.bvger.ch/dam/bvger/de/dokumente/2015/12/a-5641_2014_a-64532014zweiangestelltedersbbwegenzweckwidrigerint.pdf.download.pdf letztmals besucht am 02.02.2023
DSG	Bundesgesetz über den Datenschutz
ISO 27037:2012	ISO 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence
ISO/IEC 27043:2015	ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes
hosttech.ch	*Phishing-Attacke auf hosttech - das ist passiert!*, hosttech.ch, vom 28.08.2019, https://www.hosttech.ch/blog/phishing-attacke-hosttech letztmals abgerufen am 02.02.2023

Halbjahres-bericht 2019/1 der MELANI	https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2019-1.html letztmals abgerufen am 15.11.2019
NZZ	*Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat*, Christin Severin, vom 10.07.2019 https://www.nzz.ch/wirtschaft/cyber-angriff-auf-schweizer-firma-offix-ein-kampf-ums-ueberleben-ld.1492862 letztmals abgerufen am 02.02.2023
OR	Obligationenrecht. Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht)
RFC 3227	Guidelines for Evidence Collection and Archiving, https://tools.ietf.org/html/rfc3227, letztmals abgerufen am 15.11.2019
SKPPSC	Schweizerische Kriminalprävention, Webseite zu Stalking https://www.skppsc.ch/de/themen/gewalt/stalking/ letztmals abgerufen am 02.02.2023
StPO	Schweizerische Strafprozessordnung
Überwachung der Arbeitnehmer	*Wegleitung zur Verordnung 3 zum Arbeitsgesetz*, SECO, vom März 2013
Wikipedia zu IDS	https://de.wikipedia.org/wiki/Intrusion_Detection_System letztmals abgerufen am 02.02.2023
Wikipedia zu Turla	https://de.wikipedia.org/wiki/Turla letztmals abgerufen am 02.02.2023
Wikipedia zu Stalking	https://de.wikipedia.org/wiki/Turla letztmals abgerufen am 02.02.2023
ZPO	Schweizerische Zivilprozessordnung

Abkürzungsverzeichnis

a.a.O.	am angegebenen Ort
Abs.	Absatz
Art.	Artikel
BSI	Bundesamt für Sicherheit in der Informationstechnik https://www.bsi.bund.de/
CERT	Computer Emergency Response Team
CSiRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures https://cve.mitre.org/
etc.	et cetera
etc. pp.	et cetera perge, perge
f.	folgend
ff.	fortfolgend
HIDS	Host-based Intrusion Detection System
ISO	Internationale Organisation für Normung
lit.	litera
IT	Informationstechnik
MELANI	Melde- und Analysestelle Informationssicherung MELANI https://www.melani.admin.ch
NIDS	Network Intrusion Detection System
RAM	Random Access Memory
RFC	Request for Comments
Rz	Randziffer
S.	Seite
sog.	sogenannt
vgl.	vergleiche
Ziff.	Ziffer
z.B.	zum Beispiel

LAYER 8 GmbH
Zentralstrasse 20
Postfach 1343
CH-6031 Ebikon/Luzern

+41 41 511 5008
contact[at]layer-8.law
https://layer-8.law