Schutz vor Ransomware und Advanced Persistent Threats (APT)

LEITLINIEN FÜR PRÄVENTION, RISIKO- UND SCHADENSMINIMIERUNG

Wien, im Dezember 2016

Ransomware und Advanced Persistent Threats werden für Unternehmen zu einem immer größeren Risikofaktor. Im Rahmen der Event-Serie „collaboration for experts“ hat d-con.net daher am 9. November 2016 ein Expertentreffen zu dem Thema veranstaltet. Im Rahmen von Kurzvorträgen, Live-Demos und Diskussionen wurden die Möglichkeiten ausgelotet, mit denen sich Organisationen bestmöglich gegen die mit diesen Bedrohungen einhergehenden Risiken absichern können. Die wesentlichen Ergebnisse der Veranstaltung sind hier in kompakter Form zusammengefasst.

1. DIE BEGRIFFE RANSOMWARE UND ADVANCED PERSISTENT THREATS

Bei den Begriffen „Ransomware“ und „Advanced Persistent Threats“ handelt es sich um relativ unscharfe Schlagworte, mit denen jeweils ein Bündel von Bedrohungen mit ähnlichen Charakteristiken zusammengefasst wird. In der IT-Security Praxis liegen die beiden Bedrohungsszenarien nahe beieinander und können bezüglich Prävention und Abwehrmaßnahmen ähnlich behandelt werden. Sowohl Ransomware als auch APT infizieren den Zielcomputer mit Malware, die dann ihr Unwesen treibt:

Advanced Persistent Threats (APT) verhalten sich meistens still und sind oft auch sehr gezielt auf einzelne Organisationen gerichtet. Mittlerweile werden sie aber auch oft schon breitflächiger eingesetzt, mit ähnlichen Verbreitungsmechanismen wie Ransomware. Hauptzugang der APT ist, auf einem Computer im Hintergrund zu lauern (daher „persistent“), Informationen zu sammeln und an den Angreifer zu übertragen oder auch Sabotage auszuüben. Ein berühmtes, geradezu klassisches Beispiel für APT war die Malware Stuxnet, mit der in Iranischen Atomanlagen Sabotage betrieben wurde.

Ransomware wird für das Opfer früher oder später direkt und drastisch sichtbar. Das Wirkungsprinzip ist einfach: Auf dem befallenen Computer werden Daten verschlüsselt und in weiterer Folge wird Lösegeld verlangt. Die Ähnlichkeit zu APT liegt darin, dass auch Ransomware immer intelligenter und ausgeklügelter arbeitet, wie zum Beispiel dass es sich längere Zeit im Netzwerk einer Organisation

unsichtbar verbreitet und erst dann mit den Erpressungsaktivitäten beginnt. Das bis dato bekannteste Beispiel für Ransomware war die Schadsoftware Locky, mit der sehr erfolgreiche Erpressungsaktivitäten betrieben wurden. Derivate von Locky sind unter anderen Namen auch heute noch im Umlauf.

2. SICHERHEIT VERSUS RISIKO

Bedrohungen wie Ransomware und APT führen dazu, dass Unternehmensleitungen von ihren IT-Abteilungen mehr und mehr die Absicherung geschäftskritischer Prozesse verlangen. Was mit der Forderung „Machen Sie das sicher…“ aber allzu leicht übersehen wird, ist der Umstand, dass hundertprozentige Sicherheit nie realisierbar ist. Für einen praxisnahen Zugang beim Schutz vor modernen Bedrohungen ist es daher notwendig, klar zwischen Sicherheit und Risikominimierung zu unterscheiden: 100%ige Sicherheit ist niemals möglich, sondern nur eine wirtschaftlich vertretbare Risikominimierung. Zur Untermauerung hier ein Zitat aus dem Informationssicherheitshandbuch des Bundes:

> *„Informationssicherheit entsteht nicht von selbst aus Technik oder Know-how, sondern zunächst aus dem Bewusstsein des Managements und der MitarbeiterInnen einer Organisation, dass Informationen schützenswerte und gefährdete Werte für alle Beteiligten darstellen. Daher sind auch kontinuierliche Anstrengungen und Kosten für Informationssicherheit in Kauf zu nehmen, um sie zu erhalten. Es muss allerdings ebenso bewusst sein, dass 100% Sicherheit nicht erreicht werden kann, wie viel man auch investiert. Ziel muss es also sein, ein angemessenes Sicherheitsniveau zu erreichen und dauerhaft zu erhalten.“*

Ziel aller IT-Security Maßnahmen kann also immer nur ein möglichst hoher Sicherheitsstandard durch Risikominimierung sein. Alles andere ist Illusion.

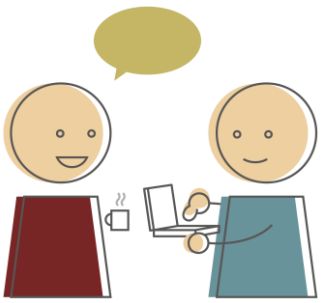
3. RISIKOMINIMIERUNG DURCH IT-SECURITY MAßNAHMEN

Gegen Ransomware und APT gibt es keinen einfachen Schutz. Wohl aber kann eine Kombination von einfachen, aber grundlegenden IT-Security Maßnahmen ein wirkungsvolles Bollwerk bilden. Werden die nachfolgend vorgestellten Maßnahmen konsequent umgesetzt, lassen sich damit viele Probleme vermeiden. Und sollte es tatsächlich zu einem Befall kommen, so bleibt der Schaden minimiert:

Empfehlung #1: Erstellen Sie eine Security Policy

Eine Security Policy alleine hilft noch überhaupt nichts und ist auch keine konkrete IT-Security Maßnahme. Wohl aber macht eine fundierte Security Policy alle weitere Umsetzungsschritte wesentlich einfacher oder überhaupt erst möglich. Denn mit der Policy wird der in der Organisation angestrebte Sicherheitsanspruch definiert. Basis einer sinnvollen Security Policy ist in jedem Fall eine gründliche Risikoanalyse – nur wenn die Risiken bekannt sind, können wirkungsvolle IT Security Grundsätze definiert werden. Wesentliche Bestandteile der Security Policy sind die Definition der Sicherheitsziele und die Festlegung der Sicherheitsstrategie, also wie die Sicherheitsziele erreicht werden. Wichtig ist, dass die Erstellung der Security Policy nicht von der IT-Abteilung ausgeht. Ganz im Gegenteil, die IT-Abteilung muss Auftragnehmer der Erstellung sein, und das Ergebnis muss von der Geschäftsleitung mit ausgearbeitet und in der Umsetzung (Enforcement, Kontrolle, Audits,...) mitgetragen werden. Einmal erstellt, sollte die Security Policy dann regelmäßig evaluiert und ggf. überarbeitet werden. Eine fertige Security Policy hilft, die richtigen Maßnahmen zu implementieren. Sie regelt auch, welche Trade-Offs (z.B. in Hinblick auf Usability, Einschränkungen beim Surfen, usw...) in Kauf genommen werden müssen um das gewünschte Sicherheitsniveau zu erzielen. Die Security Policy ist auch eine wichtige argumentative Grundlage gegenüber Lieferanten bzw. Usern. Security Policies können sich je nach Unternehmen in Art und Umfang drastisch unterscheiden. Während Konzerne mit ihrer Security Policy ganze Wikis füllen, genügen für KMUs oftmals wenige Seiten mit Aufklärungen und Arbeitsanweisungen für die IT und für die Benutzer.

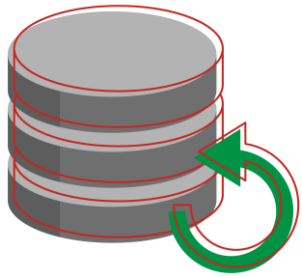
Empfehlung #2: Steigern Sie die Awareness Ihrer User



Die meisten Fälle von Ransomware wären durch ausreichende User Awareness vermeidbar. Ein wichtiger Schritt für eine Steigerung der User Awareness ist, die Security Policy intern zu kommunizieren. Ergänzend sollte es eigene Schulungen geben, wie mit verschiedenen Security Themen in der Praxis umzugehen ist. Weiters sind oft Spezialschulungen der Belegschaft sinnvoll, zum Beispiel zum Thema Ransomware und wie man sich diese am Arbeitsplatz einfängt. Manche Security Anbieter halten sogar Online-Trainings zum Thema User Awareness bereit, die für die Mitarbeiter eines Unternehmens gebucht werden können. Administratoren sind übrigens ein eigenes

Thema: Sie setzen sich erfahrungsgemäß gerne über die eigenen Richtlinien hinweg, da sie sich ja auskennen. Administratoren können oft große Probleme einschleppen, da sie zumeist mit ausgedehnten Rechten im Netzwerk unterwegs sind. Gerade bei Administratoren ist daher darauf zu achten, dass sie die Disziplin aufbringen, bei unterschiedliche Tätigkeiten mit den jeweils angemessenen Rechten zu arbeiten (Stichwort: Trennung klare Admin- und User-Accounts).

Empfehlung #3: Passen Sie Ihre Backup/Recovery Lösung an

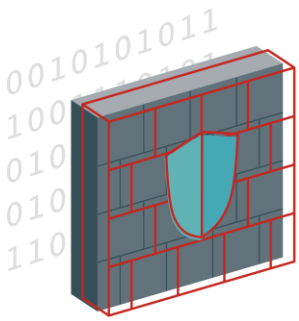


Eine gute Maßnahme zur Schadensminimierung durch Ransomware ist die Möglichkeit eines raschen Recovery. Oft stehen Unternehmen tagelang, weil die Daten auf einem Fileserver verschlüsselt wurden. Mit einer sinnvollen Backup/Recovery Strategie dagegen lässt sich ein Fileserver innerhalb kürzester Zeit wiederherstellen, es kann rasch wieder weitergearbeitet werden. Eine hohe Geschwindigkeit im Recovery Prozess ist also eine sehr effiziente Risikominimierungsmaßnahme. Daher sollte die Datenwiederherstellung nach Notfällen auch als Teil der Security Strategie mit betrachtet werden. Ebenso sind regelmäßige Tests der Backup/Recovery Lösung unerlässlich. Auch für manche Clients (z.B. Notebooks von Außendienstmitarbeitern) ist eine eigene Recovery Strategie sinnvoll. Diese Clients sind oft besonderen Risiken ausgesetzt. Auch dafür gibt es einfache Lösungen, die nur eingerichtet werden müssen. Allzu oft wird – speziell in kleinen und mittelgroßen Umgebungen – darauf vergessen, die Backups selbst vor dem Zugriff durch Bedrohungen zu schützen. So ist es zum Beispiel schon vorgekommen, dass Backups von Ransomware gleich mit verschlüsselt wurden (Beispiele: Die USB Platte bleibt am zu sichernden Rechner immer angeschlossen, Backup liegt am NAS und der Zugriff dort ist nicht ausreichend eingeschränkt, usw...).

Empfehlung #4: Nützen Sie angemessene Endpoint Protection

Eine wesentliche Basismaßnahme jeder wirkungsvollen IT-Security Lösung besteht darin, die Clients und die Fileserver selbst in sinnvoller Weise abzusichern. Dazu gehört in erster Linie ein professionelles Antivirus Produkt, die Aktivierung von Windows Defender ist bei weitem nicht ausreichend. Weiters sollte darauf geachtet werden, dass auf den Clients die Software auf dem letzen Stand ist, d.h. dass alle Patches eingespielt wurden, mit denen bekannte Sicherheitslücken z.B. im Betriebssystem oder in anderer Standardsoftware geschlossen wurden. Darüber hinaus lassen sich mit Windows Bordmitteln weitere Schritte in Richtung Endpoint Protection setzen – zum Beispiel ist es möglich, die Ausführung von Makros zu deaktivieren oder die Ausführung von EXE-Dateien einzuschränken. Wenn alle diese Möglichkeiten in einer sinnvollen Kombination genützt werden, kann die Risikolage auf den Clients selbst bereits erheblich verbessert werden.

Empfehlung #5: Schärfen Sie Ihre Perimeter Security nach



Der bloße Einsatz einer Firewall garantiert noch kein ausreichendes Sicherheitsniveau. Entscheidend ist, dass sie auch professionell genutzt wird. Denn die installierten Firewalls nehmen meistens ein Standard-Webfiltering vor, sind aber oft nicht customized, um die User nicht zu verärgern. Ihre volle Wirkung kann Perimeter Security aber erst dann entfalten, wenn die Firewall sinnvoll angepasst wird und auch deren Logs regelmäßig auditiert werden. Intensives Webfiltering führt natürlich dazu, dass für die Clients der Traffic eingeschränkt wird. Hier kann die Security Policy als argumentative Grundlage ein sehr wesentliches Instrument zur internen Durchsetzung sein. Viele Firewalls sind auch so konfiguriert, dass der Content im SSL/TLS Traffic (sprich: hauptsächlich HTTPS) nicht überprüft wird, obwohl das technisch möglich wäre. Die Funktion ist deshalb meistens deaktiviert, da mit ihrer Nutzung ungeliebter Konfigurationsaufwand einhergeht. Heute ist diese Unterlassung noch kein großes Problem – sie wird aber einen der wesentlichsten Angriffspunkte der Zukunft bilden, eben weil die meisten Organisationen die SSL Inspection nicht aktiviert haben. Eine weitere sinnvolle und oft nicht genützte Funktion ist, unerwünschte Dateitypen schon am E-Mail Security Gateway auszusortieren und nach Möglichkeit Advanced Threat Protection zu nützen. Das verlangt zwar regelmäßige Pflege, kann aber sehr stark in Richtung Risikominimierung wirken, wenn man da klug vorgeht. Ein weiteres großes Problem ist und wird noch mehr werden, dass Cloud Providern oft blind vertraut wird. Daten werden nicht verschlüsselt übertragen, heruntergeladene Daten werden nicht gescannt. Daten von Cloud Providern sollten daher am Perimeter genauso überprüft werden wie jeder andere Download aus dem Web.

4. NEUE ANSÄTZE DER IT-SECURITY HERSTELLER

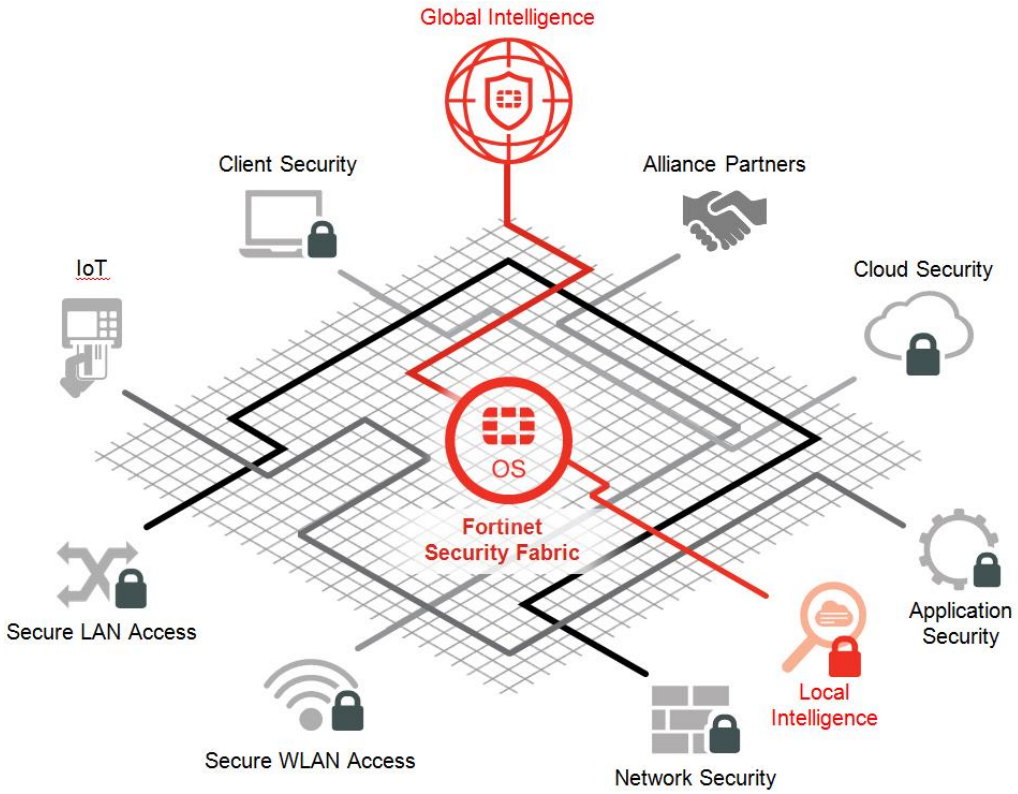
Die Hersteller von IT-Security Komponenten setzen sich natürlich intensiv mit Abwehrmöglichkeiten von Ransomware und Advanced Persistent Threats auseinander. Daraus entstehen neue Ansätze, die insgesamt einen erweiterten Zugang zur IT-Security bieten. Als Beispiel kann ein neues Konzept von Fortinet gelten, die Cooperative Security Fabric. Die Security Fabric ist ein neuer, ganzheitlicher Ansatz mit zwei wesentlichen Eigenschaften:

Integration der Security Maßnahmen

Endpoint Security, Network Security, Data Center Security, Application Security, Cloud Security, Content Security, Infrastructure Security arbeiten in der Fortinet Security Fabric Hand in Hand. Dabei werden Informationen, die in einer Funktion – oder einem Gerät – gewonnen werden, von anderen Funktionen auf unterschiedlichen Geräten vollautomatisch weiterverarbeitet. So kann zum Beispiel die Firewall auf dem Standort in Zürich einen eben erst in einer Email in Wien als „bösartig“ erkannten Link blockieren, oder die Web Application Firewall kann IP Adressen den Zugriff auf den Webserver verweigern, weil diese auf der Firewall Angriffe versucht haben.

Aufbau von Threat Intelligence

Diese Informationen werden auch als „Local Threat Intelligence“ bezeichnet, da sie lokal (in den eigenen Netzwerken) gewonnene Informationen über Bedrohungen (Threats) darstellen. Diese Informationen können noch vollautomatisch mit globalen Informationen aus der Global Threat Intelligence der FortiGuardLabs erweitert werden. Insgesamt werden mit der „Threat Intelligence“ also nicht nur Informationen aus einem globalen Kontext zur Erkennung von Sicherheitsproblemen verwendet, sondern auch sehr unternehmensspezifische.



Diese Abbildung des Security Herstellers Fortinet illustriert, dass mit der Security Fabric eine hohe Integration der einzelnen Security Maßnahmen erzielt wird. Zusätzlich ist auch die Einbindung anderer Hersteller vorgesehen.

Das Fortinet Security Fabric als Schutz gegen Ransomware und APT

Beim Schutz vor Ransomware und Advanced Persistent Threats nimmt die Fortinet Sandbox im Rahmen der Security Fabric eine zentrale Rolle ein. Alle verdächtigen Dateien, URLs, Attachments werden von den verschiedenen Geräten an die Sandbox übermittelt. Diese führt die übergebenen Dateien mit den entsprechenden Applikationen – oder Links mit einem Webbrowser - in einer virtuellen Instanz eines Client Betriebssystems aus. Während der Ausführung werden sämtliche Vorgänge auf dem virtuellen und isolierten Client überwacht und bewertet. Danach wird eine Risikoeinstufung der Datei durchgeführt und alle relevanten Informationen an alle verbundenen Geräte übermittelt. Wir beschreiben daher hier

an Hand eines Beispiels, wie einem E-Mail angefügte Malware von der Sandbox erkannt und abgefangen wird:

Angenommen, ein Client einer Fachabteilung wäre Empfänger eines E-Mails mit einem Anhang, die Malware enthält. Bei dem Anhang handelt es sich um ein Stück bis dato unbekannter Ransomware – was weder dem Benutzer bekannt wäre, noch vom Inline-Virenscanner oder seiner Endpoint Protection erkannt werden würde. Normalerweise würde das E-Mail auf dem Client landen, der Anhang würde vielleicht von dem Benutzer ausgeführt werden und die Malware würde sich dann ungehindert im Netzwerk der Organisation ausbreiten. Neu ist, dass genau das durch die Kombination von FortiMail und FortiSandbox wirkungsvoll verhindert wird. Denn noch bevor der Client das E-Mail tatsächlich erhält, wird erst der Anhang in der Sandbox auf Herz und Nieren geprüft. In diesem Fall werden verdächtige Aktivitäten entdeckt, die Zustellung des E-Mails an den Client wird verhindert und somit eine Ausführung und Verbreitung der Ransomware im Netzwerk vereitelt. Da die Sandbox durch die Security Fabric mit allen anderen Security Komponenten vernetzt ist, ist auch die Information über die neue Bedrohung sofort überall verfügbar. Die Endpoint Protection aller Clients im Netzwerk kennt ab diesem Zeitpunkt die nun nicht mehr ganz so neue Bedrohung und auch die Perimeter Security ist in der Lage, sie künftig bereits am Gateway abzufangen. Die Threat Intelligence der Organisation wurde automatisch erweitert.

Fortinet nennt diese vernetzte und intelligente Untersuchung und Behandlung von Content „Advanced Threat Protection“. Mit neuen Lösungen dieser Art lässt sich der mögliche Schaden durch Ransomware und Advanced Persistent Threats zwar nicht ganz aus der Welt schaffen, aber doch sehr deutlich minimieren. Selbst bis dato unbekannte Malware kann höchstens in einem sehr begrenzten Teil des Netzwerks aktiv sein, und das maximal für ein paar Minuten. Das ist eine entscheidende Verbesserung, da bis dato vor allem APT oft monatelang unentdeckt ihr Unwesen treiben konnten.

5. RECHTLICHE ASPEKTE

Bei dem d-con.net Expertentreffen zu Ransomware und APT am 9. November in Wien wurden auch die rechtlichen Aspekte diskutiert. Einer der Gastreferenten der Veranstaltung war Mag. Nino Tlapak von der Rechtsanwaltskanzlei Dorda, Brugger & Jordis. Nino Tlapak ist Experte für Datenschutzrecht und hat im Rahmen des Events eine Einführung in die gesetzlichen Rahmenbedingungen gegeben. Eine kurze Zusammenfassung der wesentlichen Aspekte geben wir hier wieder:

Gesetzliche Rahmenbedingung für Datensicherheit

Grundsätzlich ist in Österreich bezüglich Datensicherheit vom Gesetzgeber nur sehr wenig vorgegeben, und auch das nur in Grundzügen. Bis 2018 gilt noch das Datenschutzgesetz, das besonders technologieneutral formuliert ist, wenig konkrete Anhaltspunkte gibt und kaum Details regelt. Wesentliche Grundlage bietet der §14 des Datenschutzgesetzes: Danach ist man als Unternehmen

verpflichtet, angemessene Datensicherheitsmaßnahmen zu setzen, nach Stand der Technik und innerhalb der wirtschaftlichen Möglichkeiten. Daraus haben sich – auch aus der Judikatur – eine Reihe von Leitlinien entwickelt:

- Die Integrität, Vertraulichkeit und Verfügbarkeit von Daten muss in der Organisation gewährleistet sein.
- Die Kompetenzverteilung bezüglich der Datensicherheit muss erfolgt sein (z.B. interne Festlegung von Aufgaben und Zuständigkeiten).
- Jede Verwendung von Daten bedarf eines Auftrags oder eines Zwecks, immer in Hinblick auf Datenminimierung und Datensparsamkeit.
- Es besteht eine Belehrungspflicht, das heißt Mitarbeiter sind über Datensicherheit aufzuklären, interne Richtlinien sind herauszugeben.
- Es müssen angemessene Zutrittsberechtigungen umgesetzt werden, so dass sich nur befugte Personen im Unternehmen bewegen können.
- Für den Zugriff auf Daten müssen Betriebsbeschränkungen eingerichtet werden, so dass Mitarbeiter nur Zugriff auf Daten haben, die sie auch tatsächlich benötigen (ein besonders sensibles Thema sind z.B. Personaldaten).
- Es besteht eine Protokollierungs- und Dokumentationspflicht von Änderungen, Abfragen und Übermittlungen von Daten.

Mit der neuen Datenschutzgrundverordnung werden diese Vorgaben ab 25.5.2018 in vielen Bereichen wesentlich detaillierter und weiter verschärft.

Informationspflicht bei Datenmissbrauch

Was ist nun zu tun, wenn ein Datenmissbrauch vorliegt, zum Beispiel durch eine identifizierte Attacke durch einen Advanced Persistent Threat, mit dem Daten aus dem Unternehmen abgezogen wurden? Geregelt sind diese Fälle aktuell durch die "Data Breach Notification Duty" im §24 des Datenschutzgesetzes: Der Auftraggeber muss den Betroffenen in geeigneter Form informieren, ab Kenntnis tatsächlicher, systematischer, schwerwiegender unrechtmäßiger Verwendung von Daten (einem Datenmissbrauch) und bei drohendem Schaden für den Betroffenen. Eine Ausnahme besteht, wenn der drohende Schaden für den Betroffenen nur geringfügig ist und seine Information mit unverhältnismäßig hohem Aufwand verbunden wäre. Die möglichen Verwaltungsstrafen bei Nichteinhaltung dieser Bestimmung sind zurzeit noch relativ gering (max. EUR 10.000,-). Mit der neuen Datenschutzgrundverordnung wird sich das ab 2018 ändern, es sind dann Strafrahmen vorgesehen, die vom Unternehmensumsatz (bei Konzernen Gesamtkonzernumsatz) abhängen und in die Millionen Euro gehen können. Weiters wird es mit der neuen Datenschutzgrundverordnung ab 2018 eine Reihe von neuen Bestimmungen geben, wie zum Beispiel eine Pflicht zur Information der Aufsichtsbehörde, die binnen 72 Stunden erfolgen muss. Die Information wird auch eine Beschreibung der wahrscheinlichen Folgen sowie der ergriffenen oder vorgeschlagenen Gegenmaßnahmen enthalten müssen. Die kurze zeitliche Frist bringt mit sich, dass solche Szenarien bereits im Vorfeld durchgespielt und mögliche

Gegenmaßnahmen in der Security Policy abgebildet sein müssen. Sonst wird man kaum eine Chance haben, die Informationspflicht innerhalb der geforderten 72 Stunden einzuhalten.

Haftungsfragen bei Datenmissbrauch

Schließlich stellt sich die Frage, wer bei einem Datenmissbrauch haftet. Hier greift die Sorgfaltspflicht des Vorstandes bzw. der Geschäftsführung aus dem Aktiengesetz bzw. GmbH Gesetz. Bei schuldhafter Verletzung kommt es zu einer Schadenersatzpflicht, großes Problem in der Praxis ist die Beweislastumkehr. Das bedeutet, der Vorstand bzw. die Geschäftsleitung muss beweisen, dass sie nicht grob oder leicht fahrlässig gehandelt hat. Durch die Kontrollpflicht der Unternehmensleitung ist die Haftung auch dann ein Thema, wenn die Verantwortung für die Datensicherheit an andere Personen übertragen wurde. Für weitere Informationen zu Datensicherheitsbestimmungen, zur Informationspflicht bei Datenmissbrauch bzw. zu Haftungsfragen rund um Datenmissbrauch wenden Sie sich bitte an Mag. Nino Tlapak unter der E-Mail Adresse nino.tlapak@dbj.at. Der Experte für Datenschutzrecht steht Ihnen gerne für ein individuelles Beratungsgespräch zur Verfügung.

6. ZUSAMMENFASSUNG

Gegen Ransomware und Advanced Persistent Threats ist zurzeit kein einfacher Schutz verfügbar, wohl aber sind wirksame Vorkehrungen möglich. Die Einhaltung von wesentlichen IT-Security Grundsätzen wie die Implementierung einer Security Policy, die Pflege der User Awareness und der Aufbau einer gut funktionierenden Backup/Recovery-Lösung können ein Unternehmen erfolgreich vor dem Schlimmsten bewahren. Auf der Seite der IT-Security Hersteller gibt es neue Ansätze, die wertvolle Unterstützung gegen diese Bedrohungsszenarien bieten. Als Vorreiter kann Fortinet mit seiner Security Fabric gelten, das auch bis dato unbekannte Ransomware und APTs innerhalb einer kurzen Zeitspanne erkennt und bestmöglich isoliert. Geschäftsleitungen sollten sich auch mit den Informationspflichten und Haftungsfragen rund um erfolgte Attacken beschäftigen. Bereits jetzt bestehen eine Reihe von Pflichten und ab 2018 gelten verschärfte Bestimmungen, die empfindliche Haftungsrisiken mit sich bringen werden.

Zum Autor: Roman Rathler ist IT-Security Experte, CTO und Lead Consultant bei d-con.net. Neben seiner Projekttätigkeit bei Auftraggebern ist er auch für das Business Development des Unternehmens zuständig. Roman Rathler ist seit über 20 Jahren im Netzwerk- und Security-Bereich tätig und verfügt über tiefgehendes praktisches Know-how im Aufbau sicherer Infrastruktur.

roman.rathler@d-con.net
d-con.net GmbH
Johannesstraße 50, AT-2371 Hinterbrühl
+43 (1) 616 32 17 – 0
+43 (1) 616 32 17 – 17

d-con.net Österreich als IT-Security Anbieter

Die d-con.net GmbH mit Sitz in Österreich entwirft, plant, realisiert und betreibt IT-Infrastruktur für ihre Auftraggeber. Die wichtigsten Arbeitsbereiche des Unternehmens sind Lösungen für Netzwerke, IT-Security, Arbeitsplätze und Rechenzentren. Seine Marktstellung konnte das Unternehmen durch eine herausragende Besonderheit erlangen: Den professionellen Kooperationsstil mit Kunden, der von d-con.net in höchstem Maß gepflegt wird. Neben technischer Kompetenz sind Flexibilität, Zuverlässigkeit und Teamgeist die Säulen, auf denen der Erfolg des Unternehmens steht.

Die d-con.net Unternehmensgruppe

Die d-con.net GmbH in Österreich ist Teil der d-con.net Unternehmensgruppe mit ihren drei Gesellschaften in Österreich, Deutschland und der Schweiz. Die drei Unternehmen arbeiten eng zusammen, so dass im DACH Raum eine flächendeckende Betreuung gegeben ist. Da die d-con.net Auftraggeber oft global agierende Unternehmen sind, werden Kunden auch international in ihren Landesniederlassungen auf allen Kontinenten unterstützt. Mehr über die d-con.net Unternehmensgruppe und ihre Leistungen erfahren Sie unter www.d-con.net.