Datenschutz *konkret*

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2017

Liebe Leserin, lieber Leser,

Wie verfahren Sie eigentlich, wenn Mitarbeitende Ihr Unternehmen verlassen? Werden die E-Mail-Konten geöffnet, weitergeleitet oder direkt geschlossen? Aus Sicht des Datenschutzes ein heikles Thema, über das wir ab Seite 3 im Detail berichten.

In den letzten Wochen hat ein weiterer Erpressungstrojaner die IT-Welt erschüttert: WannaCry hat Tankstellen, Krankenhäuser, ganze Autoproduktionen stillgelegt. Die Geschichte hinter dieser Cyber-Attacke und wie Sie sich vor derartigen Angriffen schützen können, stellen wir ab Seite 8 vor.

Gern möchten wir Sie an dieser Stelle gleich auch auf die letzte Seite unseres Kundenmagazins aufmerksam machen: Wir freuen uns, zwei neue Kolleginnen bei Althammer & Kill begrüßen zu dürfen. Vor kurzem haben Frau Hörnicke und Frau Kirsch unser Team verstärkt, beide verfügen über langjährige Erfahrung in der Beratung und sind schon in ersten Projekten aktiv.

Wir wünschen wieder eine aufschlussreiche Lektüre.

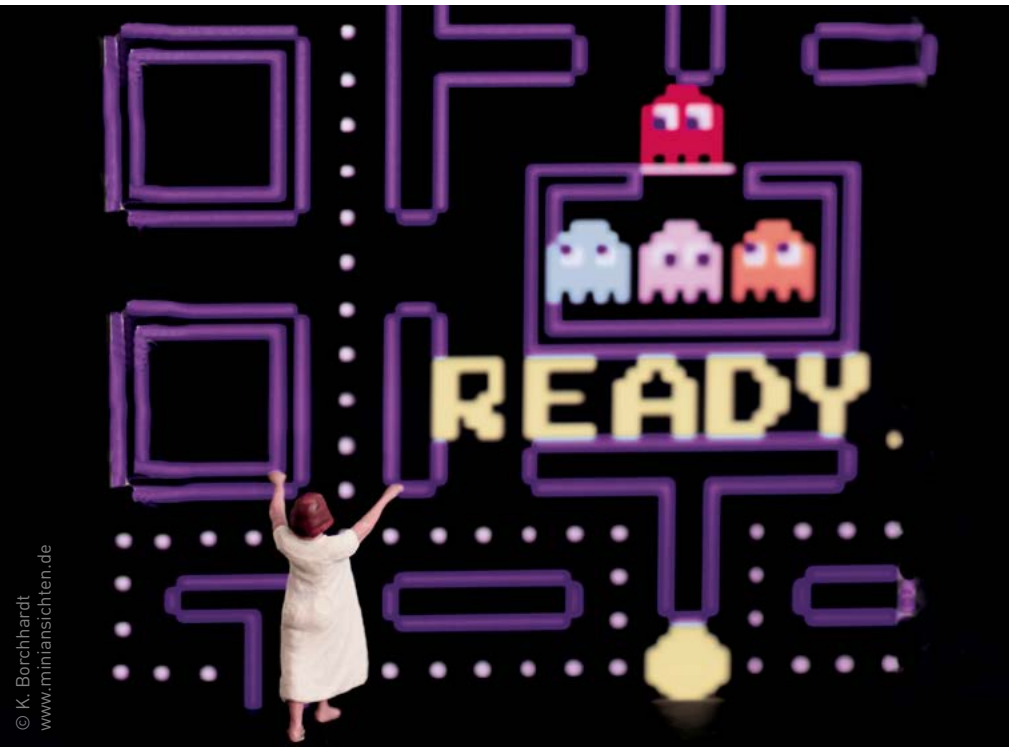
Thomas Althammer & Niels Kill

VR-Brillen: Ein Thema für den Datenschutz?

Virtual Reality (VR) ist einer der Top-Trends der Unterhaltungselektronik. Auch am Arbeitsplatz kommen bereits VR-Brillen zum Einsatz. Dabei sind nicht nur virtuelle Welten im Blick, sondern auch Sie als Nutzer.

Jeder elfte Deutsche hat bereits eine der Virtual-Reality-Brillen ausprobiert. Fast jeder Dritte kann sich vorstellen, dies künftig zu tun, so eine Umfrage des Digitalverbands Bitkom. Wenn Sie noch keine VR-Brille aufgesetzt haben: VR-Brillen präsentieren einen Bildschirm direkt vor Ihren Augen und decken das gesamte Sichtfeld ab. Dadurch schauen Sie

In dieser Ausgabe:



direkt in die Bilder und Videos und sind scheinbar Teil der virtuellen Umgebung. Selbst wenn Sie nach oben, nach unten oder zur Seite blicken: Die virtuelle Realität umgibt Sie.

Nicht nur Online-Spiele erhalten so einen neuen Erlebniswert. Es profitieren auch berufliche Anwendungen. Bitkom nennt als Beispiele Piloten, die in virtueller Umgebung die Flugzeugbedienung üben, und Ärzte, die riskante Eingriffe digital simulieren. Architekten und Städteplaner können begehbare Entwürfe erstellen. Reiseanbieter können eine Vorschau auf touristische Sehenswürdigkeiten bieten, bevor die Urlauber vor Ort sind.

Der Nutzer steht im Fokus

Bei Virtual Reality hat man als Nutzer das Gefühl, mitten im Geschehen zu sein. Auch wenn das nur virtuell ist: Tatsächlich stehen Sie als Träger einer VR-Brille im Mittelpunkt. Sie wählen das VR-Video aus, das gezeigt wird, Sie installieren die VR-Anwendungen. Mit den führenden VR-Brillen sind spezielle App-Stores verknüpft, bei denen Sie ein Nutzerprofil anlegen.

Je nach Anbieter können Sie sogar Ihr Online-Profil von Facebook oder einem anderen sozialen Netzwerk mit Ihren VR-Anwendungen verknüpfen, Ihre VR-Erlebnisse bei Facebook & Co. teilen und mit Facebook-Freunden innerhalb einer VR-Anwendung kommunizieren.

Sehen und gesehen werden

Selbst wenn Sie keine Verknüpfung zu Facebook herstellen – um ein Nutzerkonto werden Sie kaum herumkommen. Dort lässt sich protokollieren, was Sie sich angesehen haben. Tatsächlich ist es nicht nur geplant, in VR-Anwendungen passende Werbung zu machen, es geschieht schon. Dazu werden Ihre VR-Nutzungsgewohnheiten analysiert.

Mehr noch: Je nach Modell verfügt die VR-Brille über Mikrofon und Kamera, oder Sie stecken Ihr Smartphone in die VR-Brille, das über diese Funktionen verfügt. Mit Kamera und Mikrofon können Sie Kommandos geben, per Sprache oder per Blickkontakt mit der VR-Anwendung. Selbst Fotos und Videos von Ihren Erlebnissen können Sie damit machen.

Vergessen Sie aber nicht: Die Anbieter der VR-Erlebnisse könnten Sie als Nutzer analysieren, Datendiebe Sie sogar über die integrierte Kamera von Smartphone oder VR-Brille heimlich bei der Nutzung der Brille beobachten. Befassen Sie sich deshalb mit dem Datenschutz, bevor Sie in virtuelle Welten eintauchen. Denn die Datenrisiken sind real. &

Impressum

Redaktion/V. i. S. d. P.:
Niels Kill, Thomas Althammer

Haftung und Nachdruck:
Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit vorheriger Genehmigung der Althammer & Kill GmbH & Co. KG gestattet.

Anschrift:
Althammer & Kill GmbH & Co. KG
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Schutzgebühr Print-Ausgabe: 10,– €

3

Datenschutz *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2017

ALTHAMMER & KILL

Ausgeschiedene Mitarbeiter als Adressaten von E-Mails – was tun mit den Mails?

Ein Mitarbeiter scheidet aus dem Unternehmen aus. Kann der Arbeitgeber den Mail-Account des Mitarbeiters einfach schließen? Wie ist mit E-Mails umzugehen, die ausdrücklich an ihn gerichtet sind? Das Bayerische Landesamt für Datenschutzaufsicht bietet in seinem Tätigkeitsbericht für 2015/2016 einige Orientierungshilfen für diese Fragen.

Vorab sei auf Folgendes hingewiesen: Falls zu diesem Thema eine Betriebsvereinbarung existiert, ist alles klar. Es gelten ihre Regelungen. Manchmal treffen das Unternehmen und der ausscheidende Mitarbeiter auch eine ausdrückliche Vereinbarung, etwa in einem Aufhebungsvertrag. Schön für alle Beteiligten! Denn das schafft Klarheit.

Und wenn nicht?

Aber was ist, wenn es an Beidem fehlt? Vielleicht lässt sich noch über eine einvernehmliche Regelung reden. Aber manchmal erscheint das kaum vorstellbar, etwa nach einer fristlosen Kündigung. In solchen Fällen hilft die Meinung der Datenschutzaufsicht weiter.

Schließung des Mail-Accounts

Zunächst zu der Frage, wie lange ein Mail-Account noch bestehen darf. Etwa drei Monate nach dem Ausscheiden sollte er nach Auffassung des Landesamts geschlossen werden. Der Grund: Danach ist nicht mehr damit zu rechnen, dass noch Mails an den ausgeschiedenen Mitarbeiter eingehen. Eine ausdrückliche gesetzliche Regelung dazu gibt es aber nicht.

Private Nutzung erlaubt oder nicht?

Schwieriger ist eine Antwort auf die Frage, ob Mails, die noch eingehen, an einen anderen Mitarbeiter weitergeleitet werden dürfen. Hier unterscheidet das Landesamt danach, ob der Arbeitgeber die private E-Mail-Nutzung erlaubt hat oder nicht.

Falls private Nutzung verboten ist …

Relativ freie Hand hat der Arbeitgeber, wenn er die private E-Mail-Nutzung verboten hat. In diesem Fall kann er einfach festlegen, dass eine

Weiterleitung erfolgt. Denn private Mails können dann ja eigentlich keine eingehen.

Im Einzelfall kann dies aber trotzdem vorkommen. Denn immer wieder gibt es Absender, die nicht wissen, dass die private Nutzung verboten ist, oder denen das egal ist.

Umgang mit einzelnen privaten Mails

Sofern eine private Mail im Unternehmen weitergeleitet wird, darf der Empfänger ihren Inhalt nicht lesen. Das gilt naturgemäß nur dann, wenn er schon am Absender und/oder am Betreff erkennen kann, dass die Mail privaten Charakter hat. Eine solche Mail ist entweder zu löschen oder an den ausgeschiedenen Mitarbeiter weiterzusenden.

Falls private Nutzung erlaubt ist …

Falls der Arbeitgeber private Mails erlaubt hat, handelt es sich um eine freiwillige Leistung des Arbeitgebers. Das führt jedoch nicht dazu, dass er einfach die Weiterleitung aller eingehenden Mails anordnen kann. Vielmehr muss er dann das Fernmeldegeheimnis beachten.

Einwilligung nötig

Ohne eine Einwilligung des ausgeschiedenen Mitarbeiters wäre eine Weiterleitung privater Mails daher nicht zulässig. Andererseits dürfte dann auch niemand in den Account schauen, um dienstliche und private Mails zu trennen.

Das Ergebnis: Der Account wäre letztlich insgesamt blockiert. Für viele Unternehmen ist das nicht akzeptabel.

Übliche Bedingungen für private Nutzung

In der Praxis ist deshalb üblich, dass der Arbeitgeber private Mails nur unter Bedingungen erlaubt:

Bedingung 1: Der Arbeitnehmer erklärt sich damit einverstanden, dass Mails, die nach seinem Ausscheiden eingehen, an einen anderen Mitarbeiter weitergeleitet werden.

Bedingung 2: Er ist außerdem damit einverstanden, dass dieser andere Mitarbeiter den Betreff und den Absender aller eingehenden Mails prüft. Hat eine Mail danach erkennbar privaten Charakter, öffnet er sie nicht. Je nach Vereinbarung löscht er sie oder leitet sie an den ausgeschiedenen Mitarbeiter weiter.

Eigenes Smartphone als Lösung?

Falls private Mails erlaubt sind, geht es also nicht ohne relativ komplizierte Vereinbarungen. Das ist ein wichtiger Grund dafür, warum viele Unternehmen auf dienstlichen Geräten nur dienstliche Mails erlauben.

Viele Mitarbeiter haben ohnehin ständig ihr privates Smartphone dabei. Private Mails schreiben sie von dort aus. Mit den Inhalten solcher Mails hat der Arbeitgeber nichts zu tun. Datenschutzprobleme gibt es keine.

Folgeprobleme anderer Art

Allerdings: Mailen ist hier eine private Tätigkeit während der Arbeitszeit. Ob und in welchem Umfang sie erlaubt ist, sollte man klären, bevor es Ärger gibt. Selbstverständlich ist eine solche Erlaubnis auf keinen Fall.

Außerdem: Probleme kann auch der umgekehrte Fall bereiten. Ein Arbeitnehmer benutzt sein privates Smartphone, um dienstliche Mails zu verschicken. Auch das ist nicht einfach so erlaubt. &

Interne Sperrvermerke für gefährdete Kunden?

Bürger, die persönlich gefährdet sind, können von Behörden in manchen Registern „Sperrvermerke" eintragen lassen. Ihre Daten dürfen dann entweder gar nicht weitergegeben werden oder nur unter besonderen Vorsichtsmaßnahmen. Hat das Auswirkungen darauf, wie ein Unternehmen mit Daten solcher Personen umgehen darf?

© K. Borchhardt
www.miniansichten.de

Jeder, der eine Wohnung bezieht, muss sich beim Einwohnermeldeamt anmelden. Seine Daten kommen ins Melderegister. Normalerweise ist das eine völlig unspektakuläre Angelegenheit. Es gibt allerdings auch Spezialfälle. So kann es vorkommen, dass ein Polizist persönlich gefährdet ist, weil sich Kriminelle an ihm rächen wollen. Er kann dann beantragen, dass für ihn im Melderegister eine Auskunftssperre eingetragen wird. Die Sperre soll verhindern, dass seine Adresse den falschen Leuten in die Hände fällt.

Auskünfte über die aktuelle Anschrift sind ohne eine solche Sperre relativ leicht zu erhalten. Zwar muss man dabei zumindest den Namen und den Vornamen der gesuchten Person nennen können. Gerade bei seltenen Namen stellt das aber keine große Hürde dar

Auswirkungen auch auf Unternehmen?

So weit, so gut. Bis dahin ist das eine behördeninterne Angelegenheit, die Unternehmen normalerweise nicht weiter interessiert. Das ändert sich freilich sofort, wenn ein solcher Bürger mit Auskunftssperre von einem Unternehmen verlangt, ihn ebenfalls besonders zu schützen. Solche Forderungen häufen sich inzwischen.

Teils extreme Forderungen von Kunden

Manche Kunden gehen sogar so weit, dass sie verlangen, auch im Unternehmen so etwas wie eine interne Auskunftssperre zu bekommen. Sie soll bewirken, dass ganz normale Unternehmensmitarbeiter keinen Zugriff mehr auf die Daten dieses Kunden haben. Ein Zugriff soll nur noch ausgewählten, besonders vertrauenswürdigen Mitarbeitern möglich sein.

Was auf den ersten Blick durchaus nachvollziehbar wirken mag, behindert bei näherem Hinsehen die Arbeitsabläufe erheblich. Gäbe es einen solchen Anspruch, müsste die Datenverarbeitung entsprechend angepasst werden. Außerdem wären besondere Mitarbeiter auszuwählen. Also alles keine Kleinigkeiten!

Position der bayerischen Datenschutzaufsicht

Das Bayerische Landesamt für Datenschutzaufsicht hat in seinem Tätigkeitsbericht 2015/2016 klar Position bezogen, wie mit solchen Forderungen umzugehen ist. Es hebt Folgendes hervor:

- Unternehmen dürfen Daten ohnehin nur verarbeiten, wenn dies für die Tätigkeit des Unternehmens erforderlich ist.

- Ist diese Voraussetzung gegeben, dürfen alle Mitarbeiter Zugriff auf die Daten erhalten, die sie für ihre Arbeit brauchen. So muss etwa die Buchhaltung auf die Daten aller Kunden zugreifen können, bei denen noch eine Rechnung offen ist.

- Zugriffsbeschränkungen, die darüber hinausgehen, kann kein Kunde

verlangen. In den Datenschutzgesetzen, die für Unternehmen gelten, gibt es keine Regelungen über so etwas wie Sperrvermerke oder Auskunftssperren.

– Ist im Register einer Behörde ein Sperrvermerk, eine Auskunftssperre oder etwas dergleichen eingetragen, dann hat dies nur für die Arbeit dieser Behörde Bedeutung. Auswirkungen auf Unternehmen ergeben sich dagegen nicht.

Vorsicht vor Überinterpretationen!

Dies ist eine wichtige Klarstellung. Sie darf allerdings auch nicht überinterpretiert werden. So kann Folgendes vorkommen:

– In einem Einwohnermelderegister ist für einen Bürger eine Auskunftssperre wegen Gefährdung eingetragen.

– Ein Unternehmen möchte vom Einwohnermeldeamt die aktuelle Anschrift dieses Bürgers erfahren. Der Grund: Es ist noch eine Rechnung offen, und der Bürger ist umgezogen, ohne dem Unternehmen seine neue Anschrift zu melden.

– Erst nach einigen Wochen teilt die Behörde die aktuelle Anschrift schließlich mit. Dabei macht sie allerdings eine besondere Auflage. Sie legt fest, dass die Anschrift nur für den Zweck verwendet werden darf, um den es bei der Anfrage ging. Das ist gewissermaßen der Preis dafür, dass das Unternehmen die Anschrift erhält, obwohl eine Auskunftssperre eingetragen ist.

Erst denken, dann Daten weitergeben!

Folge für die Praxis: Die Adresse darf nur zu dem Zweck verwendet werden, den Kunden wegen der konkreten Rechnung anzusprechen. Unzulässig wäre es dagegen, ihm beispielsweise Werbung an diese Adresse zu schicken. Und dass jegliche Weitergabe der Anschrift an Stellen außerhalb des Unternehmens verboten ist, versteht sich von selbst.

Das gilt auch, wenn „befreundete Unternehmen“ anfragen, die ebenfalls nach der aktuellen Anschrift suchen. &

Eine bange Frage: Bin ich ein Innentäter?

Innentäter gelten als eines der größten Risiken für die Datensicherheit in Unternehmen. Nicht die Hacker von außen verursachen die meisten Vorfälle, sondern die sogenannten Insider. Gehören Sie auch dazu?

Sicherlich haben Sie in den Nachrichten schon einmal von Insider-Handel gehört. Bei diesem Vergehen geht es darum, dass jemand sein internes Wissen dazu missbraucht, um Vorteile beim Kauf oder Verkauf von Wertpapieren zu erzielen. Auch im Datenschutz gibt es Insider-Wissen, im Prinzip hat dies jede Mitarbeiterin und jeder Mitarbeiter, der mit personenbezogenen Daten umgeht, also zum Beispiel mit Kundendaten. Zusätzlich haben Insider Berechtigungen, Daten zu lesen, zu ändern oder zu löschen. Werden diese Berechtigungen missbraucht, spricht man von einer Insider-Attacke.

Keine Sorge, niemand will Ihnen nachsagen, dass Sie eine Insider-Attacke planen oder so etwas jemals getan hätten. Doch vielleicht sind Sie trotzdem ein Innentäter, ohne es zu wissen oder zu ahnen.

Innentäter sind es meist ohne Vorsatz

Die meisten Insider-Vorfälle resultieren aus Nachlässigkeit oder Unwissenheit: So enthalten beispielsweise rund 16 Prozent der Dokumente, die in einer Cloud, also einem Online-Datenspeicher abgelegt werden, sensible Informationen, so eine Studie von Skyhigh Networks.

Diese Dateien dürften deshalb nie in einen ungeschützten Online-Speicher kopiert werden, aber es passiert trotzdem. Durch falsch definierte Zugriffsberechtigungen stehen einige dieser Dokumente dann sogar noch der breiten Öffentlichkeit zur Verfügung. Das geschieht zwar nicht

mit Absicht. Es kann aber schwerwiegende Konsequenzen haben.

Fahrlässige Nutzer: ein großes Risiko

Unternehmen sehen laut einer Splunk-Umfrage derzeit die größten Risiken in

- Computer-Viren (67 Prozent),
- hochentwickelten, andauernden Bedrohungen (Advanced Persistent Threats) (42 Prozent),
- Phishing-Attacken (28 Prozent) und
- fahrlässig handelnden Nutzern (27 Prozent).

Das können Nutzer sein, denen persönliche Zugangsdaten entwendet wurden. Diese Nutzer haben sich dann nicht gut genug geschützt und interne IT-Sicherheitsrichtlinien nicht eingehalten. Solche Nutzer werden ungewollt zu Gehilfen der Hacker und Datendiebe.

Denken Sie an Selbstdatenschutz und die internen Vorgaben

Tatsächlich ist so manche Mitarbeiterin und so mancher Mitarbeiter Innentäter, ohne wirklich Täter zu sein. Ungewollt machen sie es den echten Tätern, den Datendieben, aber leicht, an die zu schützenden Daten zu kommen.

So werden Daten nicht verschlüsselt, bevor sie auf einem USB-Stick gespeichert werden, oder das Firmen-Smartphone ist so eingestellt, dass das Gerätepasswort nicht mehr eingegeben werden muss, da dies lästig erschien.

Oder Mitarbeiter holen vertrauliche Ausdrucke nicht vom Drucker ab. Gedruckte Kundenlisten landen im Papierkorb und nicht im Papier-Schredder. Die Liste möglicher Fehler ließe sich beliebig fortsetzen.

Wichtig ist es, dass Sie sich immer klarmachen, dass Sie zum Innentäter werden könnten, ohne es zu wollen, dadurch es aber den Datendieben ermöglichen, schnell und einfach an die Daten der Kunden, Lieferanten oder Beschäftigten zu kommen.

Denken Sie deshalb an den Selbstdatenschutz, werden Sie aktiv, indem Sie Ihre Daten und die der anderen schützen. Was genau zu tun ist, erfahren Sie in der Datenschutzschulung und in den Datenschutzrichtlinien.

Wenn Sie sich daran halten, können Sie mit Fug und Recht sagen: Ich bin kein Innentäter, ich schütze mein Insiderwissen und trete aktiv für den Datenschutz ein! Gut so! &

Kennen Sie die Gefahren einer Virtuellen Realität (VR)? Machen Sie den Test!

Frage: Mit VR-Brillen schaut man sich Scheinwelten an, echte Gefahren lauern dort nicht. Stimmt das?

a. Ja, denn VR steht für Virtuelle Realitäten, die echte Welt hat damit nichts zu tun.
b. Nein, denn die VR-Brille selbst ist eine echte Realität. Stimmt hier der Datenschutz nicht, bestehen Datenrisiken.

Lösung: Die Antwort b. ist richtig. Überall im Internet und in Apps können Datenrisiken stecken. Das gilt auch für VR-Apps. Der Bildschirm der VR-Brille präsentiert virtuelle Welten, doch die Brille, die Apps und die Nutzerdaten sind real und deshalb gefährdet.

Frage: Was ich in der VR-Brille anschaue, sehe nur ich. Stimmt das?

a. Nein, denn Dritte können die VR-Nutzung auswerten.
b. Nein, Dritte könnten versuchen, auf die Kamerafunktion zuzugreifen.
c. Ja, denn die VR-Brille schließt dicht ab, keiner kann auf meinen Bildschirm darin schauen.

Lösung: Die Antworten a. und b. sind richtig. Die VR-Brille erscheint abgeschlossen, doch es besteht Verbindung zu den Apps, zum Internet und zum Nutzerkonto. Die VR-Nutzung lässt sich auswerten, die Verbindung zu den VR-Apps kann ausspioniert werden, wenn Datenschutz und Datensicherheit nicht stimmen. VR-Anwendungen brauchen den gleichen hohen Schutz wie mobile Apps und VR-Brillen die gleiche Sicherheit wie mobile Endgeräte. Sonst sieht man als Nutzer nicht nur virtuelle Welten, sondern man wird womöglich auch selbst von Dritten über das Internet gesehen und analysiert.

Wie schütze ich mich vor Erpressungstrojanern?

WannaCry-Cyberattacke sorgt für Ausfälle bei Tankstellen, Krankenhäusern und der Deutschen Bahn

Anzeigetafeln der Bahn zeigen Erpressernachrichten, mehr als 20.000 Tankstellen sind offline. Nach mehr als 200.000 infizierten Computern in 150 Ländern stoppt ein 22-jähriger Sicherheitsexperte die weitere Verbreitung.

Nach Locky & Co. kursierte ab Freitag dem 12.05.2017 ein neuer Erpressungstrojaner mit dem Namen „WannaCry“. Binnen kurzer Zeit waren Tankstellen, Kliniken, Anzeigetafeln an Bahnhöfen betroffen. Selbst die Autoproduktion bei Renault-Nissan musste gestoppt werden.

Das Virus konnte sich über eine ungepatchte Sicherheitslücke in älteren Microsoft Windows-Systemen rasch verbreiten.

Als hätten wir nicht schon genug durch die Cyberangriffe der letzten Jahre gelernt

Die immensen Auswirkungen hätten sich vermeiden lassen: Microsoft hatte im März einen Patch bereitgestellt, das aber noch nicht von allen Anwendern installiert wurde. Dabei mahnen Sicherheitsexperten seit Jahren, Betriebssysteme und Software stets aktuell zu halten, um derartige Angriffe zu verhindern.

Kill Switch per Zufall entdeckt

Ironie des Schicksals: der Virus selbst verfügte ebenfalls über eine Art „Sicherheitslücke“. So fand ein britischer Sicherheitsexperte bei der Analyse des Verschlüsselungstrojaners Hinweise auf eine Internet-Domäne. Er registrierte diese kurzerhand, was die weitere Verbreitung abrupt stoppte: jeder befallene Rechner meldet sich nun unter dieser Adresse. Es handelt sich dabei scheinbar um eine

Art „Kill-Switch“, der in diesem Fall nicht sonderlich gut versteckt war.

Gegenmaßnahmen? Auch die Regierungen sind gefordert

Laufend Updates, Virenschutz mit APT-Funktionen, E-Mail-Schutzsysteme, extreme Vorsicht, Netzwerksegmentierung, usw. usw. All dies sind Sicherheitsmaßnahmen die helfen, derartige Attacken möglichst glimpflich ausgehen zu lassen.

Interessant ist in diesem Fall ein Blog-Beitrag von Microsoft. Die Sicherheitslücke wurde zunächst vom US-Geheimdienst NSA entdeckt und für Spionage-Tätigkeiten genutzt. Vor kurzer Zeit wurde sie durch Unbekannte publik und damit zu einer akuten Bedrohung. Die gewünschte Geheimhaltung hat in diesem Fall nicht funktioniert und wurde damit binnen kürzester Zeit zu einem weltweiten Problem – auch für Teile unserer kritischen Infrastrukturen.

Potentiell kann jeder betroffen sein – Datensicherung beugt vor

Es gibt ständig neue Bedrohungen und Angriffsvektoren, die potentiell jedes Unternehmen betreffen. Dabei gilt es, eine Doppelstrategie zu verfolgen: Zum einen sind Angriffe von außen laufend im Blick zu behalten und möglichst abzuwehren. Da das aber möglicherweise nicht verhindert werden kann, sind die Folgen eines potentiell erfolgreichen Angriffs zu prüfen und einzudämmen.

Die Notwendigkeit eines Backups ist dabei unbestritten. Um sich zum Beispiel nach einem Ransomware-Befall zu helfen, ist ein vorhandenes Backup oft die letzte Möglichkeit einen größeren Schaden abzuwehren.

67 % der Befragten sind sich nicht sicher, ob ihre Backups zurückgespielt werden können!

Unabhängig von der Größe der jeweiligen Infrastruktur (ob nur ein oder mehrere Server oder gar ein Rechenzentrum) ist das Backup schon seit Beginn der Informationstechnologie eine unverzichtbare aber auch zugleich ungeliebte Aufgabe. Unverzichtbar, weil auch IT-Systeme nicht vor einem Defekt gefeit sind und unbeliebt, weil man sich mit etwas beschäftigen muss, was höchstens dafür sorgt, dass ein Zustand wiederhergestellt wird, den man eigentlich schon einmal hatte.

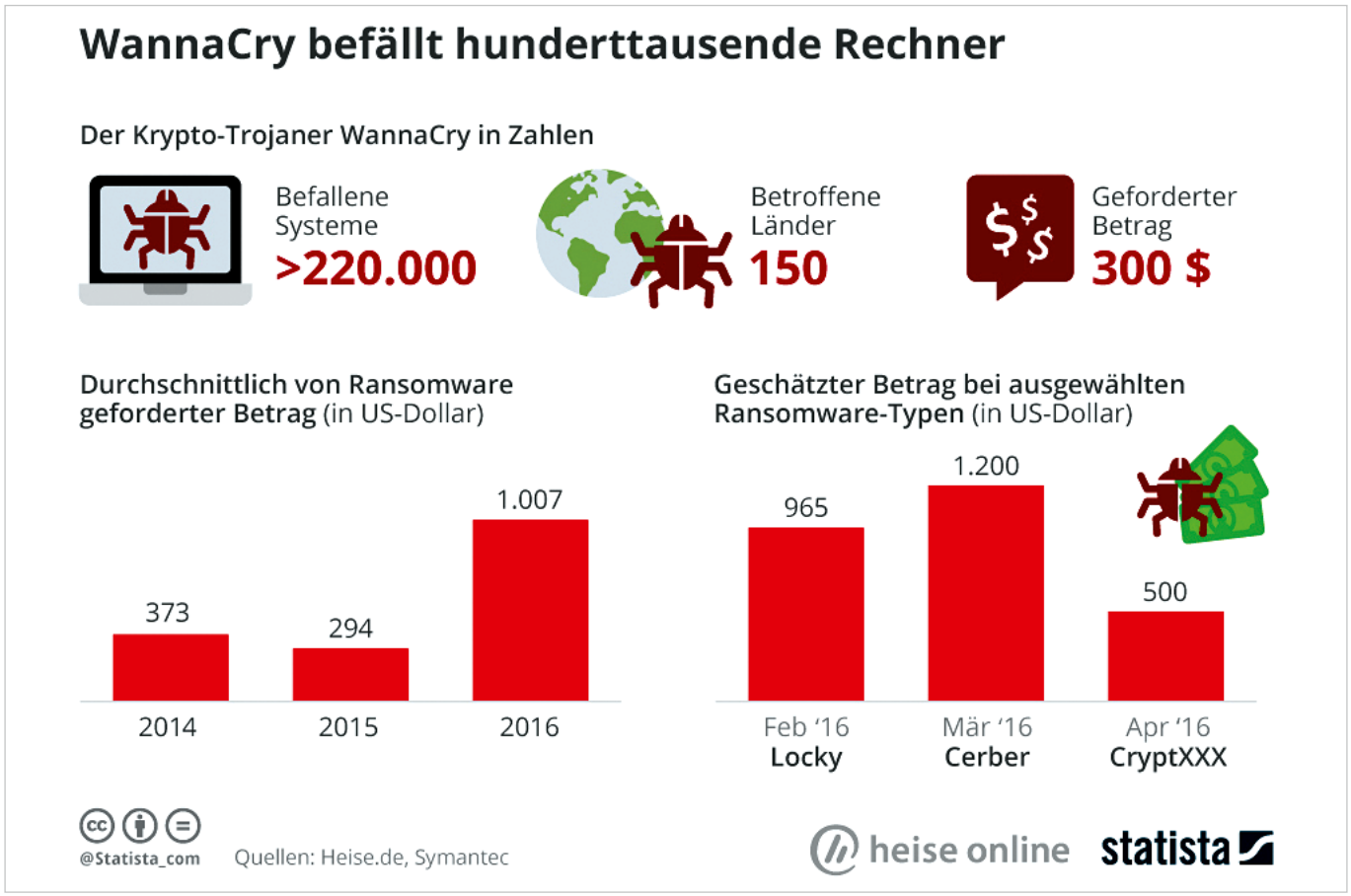
Zudem hofft man, dass der Fall nie eintritt. Das führt dazu, dass die Aufgabe oft als weniger dringlich angesehen und immer wieder verschoben wird. Wenn dann der Fall der Fälle doch eintritt, ist es dann meistens zu spät.

Während man bei einem technischen Versagen vielleicht noch etwas retten kann, besteht bei einem Ransomware-Befall meistens wenig Hoffnung.

In einem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten Leitfaden zum Umgang mit Erpressersoftware, werden nicht nur Abwehrmaßnahmen aufgezeigt, sondern es werden auch empfohlen Präventivmaßnahmen aufgezeigt. Einen aktuellen IT-Notfallplan zu haben und eben ein funktionierendes Backup sind einige der empfohlenen Maßnahmen.

Datensicherung lokal, bei einem Dienstleister oder in der Cloud?

Ein von der Initiative „Cloud Service made in Germany“ durchgeführte Umfrage stellt dar, das ca. 90 % der Befragten nach eigenen Angaben über funktionierende Maßnahmen zur Datensicherung und -Wiederherstellung verfügen. 67 % Prozent der Befragten waren sich jedoch nicht sicher, ob sie nach einem Ausfall alle



Backup-Daten tatsächlich korrekt zurückspielen könnten.

Vielfach – gestern wie heute - wird auf Tapes gesichert. Diese Methode (insbesondere was die Haltbarkeit des Speichermediums betrifft) ist immer noch beliebt. Einzig die schiere Menge der zu sichernden Daten sorgen hier oft für (Kapazitäts-) Probleme. Mittlerweile gibt es auch andere Backup-Möglichkeiten.

Neben der lokalen Datensicherung bietet sich z. B. die Sicherung bei einem Dienstleister oder sogar in der Cloud an. Daraus leiten sich mehrere Anforderungen ab. Erstens sollten sie einfach zu warten sein. Diesbezüglich lohnt sich die Überlegung, ob man auf eine reine Software setzt oder zu einer Appliance greift. Zweitens stellt sich die Frage, wohin gesichert werden soll? Lediglich auf ein anderes Gerät? In ein anderes Rechenzentrum oder soll man den Trend zum Backup-as-a-Service respektive dem Backup bei einem Anbieter von günstigem Cloud-Speicher folgen?

Wird ein Cloud-Backup in Erwägung gezogen, dann gilt es auch darüber nachzudenken, wie sichergestellt wird, dass sich keine zu großen Abhängigkeiten ergeben. Amazon (AWS) oder Google unterstützen zwar viele, insbesondere US-amerikanische Produkte zur Datensicherung, aber möglicherweise will oder kann man diese Dienste nicht nutzen, z. B. weil diese gegen hiesige Datenschutzvorschriften verstoßen.

Sofern man sich für die Datensicherung an einem zweiten Standort oder in der Cloud entscheidet, kommt früher oder später die Frage nach der Optimierung der Datenübertragung über die WAN-Strecke auf. Hilfreich ist da natürlich die auch für lokale Sicherungen schon bewährte Deduplizierung. Damit lässt sich das Datenvolumen oft schon auf ein Zehntel reduzieren. &

Benötigen Sie weitere Informationen?

Sie haben Fragen zu Backup- und Recovery, Datensicherungskonzepten oder zur Konzeption von IT-Notfallplänen? Gern unterstützen wir Sie bei deren Beantwortung:

info@althammer-kill.de

Termine

Wir freuen uns auf persönliche Begegnungen –
zum Beispiel im Rahmen der folgenden Veranstaltungen:

20.06.2017–22.06.2017, Paderborn
Ausbildung Datenschutzbeauftragte Fokus Kirche & Sozialwirtschaft
Grundlagenseminar Datenschutz auf Basis von BDSG, DSG-EKD und KDO.

21.06.2017, Hannover
Die neue Datenschutz-Grundverordnung (DS-GVO)
Durch die Verabschiedung der neuen DS-GVO ändert sich die datenschutzrechtliche Situation in Deutschland. In unserem Seminar lernen Sie den Status quo von Änderungen, Auswirkungen und Umsetzung kennen.

22.06.2017, Hannover
EU-US Privacy Shield – Auswirkungen und Fallstricke für den Mittelstand
Das Seminar informiert mit hohem Praxisbezug über Möglichkeiten und Grenzen von Privacy Shield.

07.08.2017–11.08.2017, Bielefeld
WISSEN WAS RECHT IST
Sommerakademie an der Fachhochschule der Diakonie.

12.09.2017, Paderborn
Privacy by Design: Datenschutz nimmt Anbieter und Administratoren stärker in die Pflicht
Spätestens mit der EU Datenschutz-Grundverordnung (DS-GVO) sollten Unternehmen bereits bei der Auswahl von IT-Lösungen berücksichtigen, inwieweit diese datenschutzrechtlichen Anforderungen genügen.

Termin verpasst? Anruf oder E-Mail genügt und wir lassen Ihnen gern weitere Informationen zukommen.

News

Aus unserem aktuellen Newsletter:

„Datenschützer sind Menschenrechtsbeauftragte“
https://www.althammer-kill.de/news-detail/datenschuetzer-sind-menschenrechtsbeauftragte/

Datensicherung in Unternehmen
https://www.althammer-kill.de/news-detail/datensicherung-in-unternehmen-292/

Was machen eigentlich Aufsichtsbehörden für den Datenschutz?
https://www.althammer-kill.de/news-detail/was-machen-eigentlich-aufsichtsbehoerden-fuer-den-datenschutz/

Gesundheitsdaten sind wertvoller als Finanzdaten!
https://www.althammer-kill.de/news-detail/gesundheitsdaten-sind-wertvoller-als-finanzdaten/

Der gläserne iPhone Nutzer: Vom großen Bruder in der Hosentasche
https://www.althammer-kill.de/news-detail/der-glaeserne-iphone-nutzer-vom-grossen-bruder-in-der-hosentasche/

Neuregelung § 203 StGB: Wird die Schweigepflicht reformiert?
https://www.althammer-kill.de/news-detail/neuregelung-203-stgb-wird-die-schweigepflicht-reformiert/

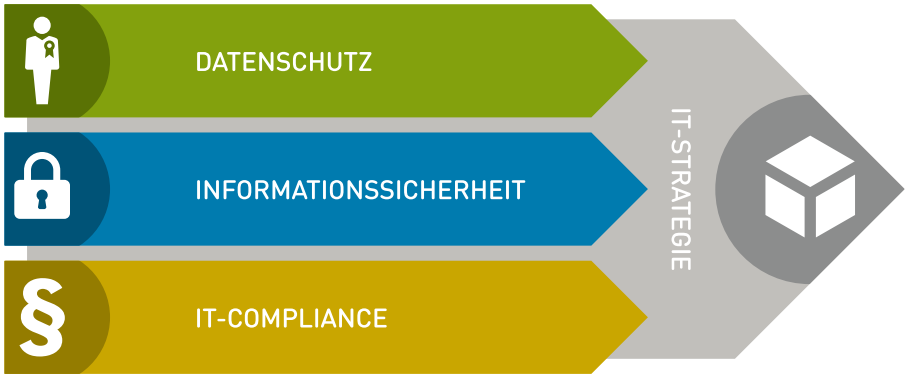
Anmeldemöglichkeiten zu unserem Newsletter finden Sie unter:
www.althammer-kill.de

12 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2017

ALTHAMMER & KILL

Althammer & Kill – Wir schützen Ihre Daten.

Althammer & Kill ist ein auf Datenschutz, Informationssicherheit und IT-Compliance spezialisiertes Unternehmen. Unsere Mitarbeiter sind zertifizierte Datenschutzbeauftragte, IT-Sicherheitsexperten, ausgebildete IT-Compliance-Beauftragte und IT-Berater.



Datenschutz

Durch unsere langjährige Erfahrung in unterschiedlichsten Branchen können wir praxisgerechte Lösungen für Ihr Unternehmen entwickeln. Sei es im Rahmen eines konkreten Projektes oder als langfristige Begleitung Ihres Unternehmens z. B. in der Funktion als externer Datenschutzbeauftragter.

Informationssicherheit

Sind Ihre Systeme sicher? In unserer vernetzten Welt fällt es immer schwerer, den Durchblick zu behalten. Angriffe von außen oder ungewollter Informationsverlust: die Risiken sind vielfältig. Wir begleiten Sie zu Security-Fragen, prüfen die Sicherheit Ihrer Systeme und stellen den IT-Sicherheitsbeauftragten.

IT-Compliance

Gesetze, Verordnungen, Normen – da fällt es nicht immer leicht, Compliance-Verstöße zu verhindern. Wir begleiten branchenorientiert und liefern passende Konzepte für einen rechtssicheren Betrieb Ihres Unternehmens, z. B. im Rahmen des Risiko- und Notfallmanagements.

IT-Strategie

Welche Ziele möchten Sie mithilfe der Informationstechnologie in Ihrem Unternehmen erreichen? Wo liegen Möglichkeiten, Nutzen und Wertschöpfung? Wir orientieren unsere Arbeit an Ihren Zielen und begleiten bei der Auswahl und Gestaltung passender Strategien.

Wir sind Mitglied der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), des Berufsverbandes der Datenschutzbeauftragten Deutschlands e. V. (BvD) und des Fachverbands Informationstechnologien in Sozialwirtschaft und Sozialverwaltung e. V. (FINSOZ). &

Niels Kill
Geschäftsführer
Tel. +49 211 936748-20
nk@althammer-kill.de

Thomas Althammer
Geschäftsführer
Tel. +49 5139 973949-2
ta@althammer-kill.de

Katja Borchhardt
Organisation & Marketing
Tel. +49 211 936748-0
kb@althammer-kill.de

Mariusz Bucki
Berater für IT-Sicherheit u. Datenschutz
Tel. +49 211 936748-30
mb@althammer-kill.de

Andreas Hellmann
Berater für Datenschutz u. IT-Sicherheit
Tel. +49 211 936748-34
ah@althammer-kill.de

Daniela Hörnicke
Beraterin für Datenschutz
Tel. +49 5139 973949-6
dh@althammer-kill.de

Dr. Jan Holling
Berater für Datenschutz
Tel. +49 5139 973949-4
jh@althammer-kill.de

Frank Keusemann
Fachkraft für Arbeitssicherheit
Tel. +49 211 936748-60
fk@althammer-kill.de

Elke Kirsch
Beraterin f. Datenschutz u. IT-Sicherheit
Tel. +49 5139 973949-5
ek@althammer-kill.de

Andreas Klostermann
Berater für IT-Sicherheit
Tel. +49 211 936748-0
ak@althammer-kill.de

Althammer & Kill GmbH & Co. KG

www.althammer-kill.de
info@althammer-kill.de

Hauptsitz Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Standort Hannover:
Buchenhain 15 · 30938 Burgwedel
Tel. +49 5139 973949-0 · Fax -9