Datenschutz konkret

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 5/2016

Liebe Leserin, lieber Leser,

die Enthüllungen von Edward Snowden im Jahr 2013 waren noch lange nicht alles. Wie kürzlich bekannt wurde, soll Yahoo ab 2015 im Auftrag des US-Geheimdienstes 500 Millionen E-Mail-Konten systematisch überwacht haben.

Der Vorfall verdeutlicht, in welchem Ausmaß Überwachung heute stattfindet. Mit diesen Beispielen im Hinterkopf ist es uns Datenschutzbeauftragten nicht möglich, einer Übermittlung von personenbezogenen oder gar vertraulichen Daten in die USA bedenkenlos zuzustimmen. Damit stoßen wir oft auf Unverständnis, gerade in international agierenden Unternehmen.

Das EU-US-Privacy Shield ist hier ein erster Ansatz, aber noch weit entfernt von einer befriedigenden Lösung. Ohne weitreichende Verschlüsselung wird es nicht gehen. Unsere Beiträge gleich hier auf Seite 1 und ein Produktbeispiel ab Seite 9 zeigen auf, wie zumindest auf dem Transportweg E-Mails vor fremden Blicken geschützt werden können. Wir wünschen eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

Einfaches Schlüsselmanagement: Der Schlüssel für mehr Datenschutz

Nicht die E-Mail-Verschlüsselung an sich ist kompliziert. Sondern der richtige Umgang mit digitalen Schlüsseln, die eingerichtet werden müssen. Das Projekt Volksverschlüsselung will dabei helfen.

Grundlage für die E-Mail-Verschlüsselung schaffen

Das Bundesministerium des Innern begrüßt den Start der sogenannten Volksverschlüsselung, so war es im Sommer 2016 zu lesen. Deutschland sei auf dem Weg zum Verschlüsselungsstandort Nr. 1. Es lohnt sich

In dieser Ausgabe:

also, die Volksverschlüsselung kennenzulernen, wenn Sie sie noch nicht kennen (www.volksverschluesselung.de). Dabei werden Sie jedoch feststellen, dass die Volksverschlüsselung gar nicht selbst verschlüsselt.

Was aber macht sie dann? Die Volksverschlüsselung ist eine Software, die die notwendigen digitalen Schlüssel erzeugt und die E-Mail-Programme der Benutzer konfiguriert. Für die eigentliche Verschlüsselung brauchen die meisten Nutzer kein neues Programm, da die meisten E-Mail-Programme von Haus aus verschlüsseln können, wenn Schlüssel vorhanden sind. Somit können selbst unerfahrene Nutzer verschlüsselte E-Mails verschicken, so die Projektbeschreibung.

Hilfe bei der Schlüsselverwaltung

Verschlüsselungslösungen für E-Mails gibt es reichlich, darunter auch viele kostenlose. Die Gründe, warum viele Nutzer die E-Mail-Verschlüsselung häufig nicht einsetzen, liegen woanders: 64 Prozent der von dem Digitalverband Bitkom befragten Nutzer sagen, dass sie sich damit nicht auskennen. Kompliziert ist dabei nicht etwa das Verschlüsseln selbst. Das klappt auf Knopfdruck und lässt sich sogar automatisieren.

Schwierigkeiten bereitet den Nutzern vielmehr, die E-Mail-Verschlüsselung einzurichten.

Wahrscheinlich werden Sie zustimmen, dass es nicht einfach auf der Hand liegt, wie man an einen digitalen Schlüssel zur Verschlüsselung kommt, wie man ihn mit seinem E-Mail-Programm verknüpft und wie man den Kommunikationspartnern seinen öffentlichen Schlüssel bekannt gibt, während der private Schlüssel dauerhaft vertraulich bleiben muss. Unterstützung ist hier wirklich sinnvoll.

Das Ziel: Mehr Sicherheit bei E-Mails

Eine Lösung wie die Volksverschlüsselung kann in Zukunft helfen, auch wenn Sie privat verschlüsselt per E-Mail kommunizieren wollen. Bisher profitieren aber erst Windows-Nutzer von der Volksverschlüsselung, wenn sie über E-Mail-Programme wie Outlook oder Thunderbird kommunizieren. In weiteren Schritten sind Versionen für andere Betriebs-systeme wie Mac OS X, Linux, iOS und Android geplant.

Die Volksverschlüsselung muss noch erweitert werden. Aber sie zeigt bereits: Ist das Problem des Schlüsselmanagements erst einmal gelöst, gibt es keinen Grund mehr, den Aufwand zu scheuen. Dann wird E-Mail endlich sicherer. &

Impressum

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

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

Schutzgebühr Print-Ausgabe: 10,– €

Ein Blick in die eigenen Behandlungsunterlagen

Meist bekommt man als Patient durchaus Einsicht in die Unterlagen über die eigene Behandlung. Aber falls es doch einmal Konflikte gibt: Welche Spielregeln gelten dann eigentlich?

Behandlungsunterlagen dienen dem Patienten wie dem Arzt. Der Arzt braucht sie als Gedankenstütze. Manchmal benötigt er sie auch, um Vorwürfe wegen falscher Behandlung abzuwehren.

Funktion von Behandlungsunterlagen

Der Patient wiederum will die Unterlagen vorlegen, wenn er einen anderen Arzt aufsucht. Vielleicht möchte er sich aber auch nur informieren, was gesundheitlich eigentlich mit ihm los ist. Dann können Behandlungsunterlagen eine hoch spannende Lektüre sein.

Regelungen zu ihrem Inhalt

Was in Behandlungsunterlagen eines Arztes stehen muss, ist gesetzlich geregelt. Enthalten sein müssen sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse. So legt es § 630f des Bürgerlichen Gesetzbuchs (BGB) fest.

Aus der Sicht eines medizinischen Laien mag die Formulierung etwas schwammig wirken. Aus der Sicht eines medizinischen Fachmanns sieht das schon anders aus. Außerdem hat die etwas weite Formulierung einen wesentlichen Vorteil: Neue fachliche Erkenntnisse dazu, was in Behandlungsunterlagen hinein gehört, lassen sich recht schnell umsetzen. Das Gesetz muss dazu nicht geändert werden.

Diagnosen, Befunde, Therapien

Das Gesetz nennt konkrete Beispiele dafür, was auf jeden Fall in die Unterlagen hinein gehört, nämlich

- die Anamnese (also die medizinische Vorgeschichte des Patienten),
- ferner Diagnosen,
- Untersuchungen,
- Untersuchungsergebnisse,
- Befunde,
- Therapien und ihre Wirkungen,
- Eingriffe und ihre Wirkungen,
- Einwilligungen und Aufklärungen.

Besonders wichtig für den Patienten: Arztbriefe sind auf jeden Fall in die Patientenakte aufzunehmen.

Rechtsanspruch auf Einblick

Oft ist die Rede davon, dem Patienten werde Einblick in die Behandlungs-

Datenschutz-Siegel für Connext-Vivendi

Die Firma Connext aus Paderborn hat erfolgreich eine Datenschutz-Zertifizierung auf Basis der „Orientierungshilfe Informationssysteme im Sozialwesen“ (kurz OH-SOZ) durchlaufen. In einer Reihe von Workshops und Audits wurde das Programm auf Herz und Nieren überprüft. Zahlreiche Verbesserungen und neue Datenschutz-Funktionen wurden daraufhin in den vergangenen Monaten freigegeben.

Althammer & Kill zertifiziert Software auf Grundlage der OH-SOZ

Das Zertifikat unterstreicht, dass die Anforderungen an eine datenschutzkonforme Programmgestaltung („Privacy by Design“) und eine datenschutzgerechte Grundkonfiguration („Privacy by Default“) erfüllt sind. Dabei wurden die Anforderungen des BDSG, der LDSG und der kirchliche Datenschutz nach DSG-EKD und KDO berücksichtigt.

Vivendi-Kunden können ab sofort den datenschutzkonformen Einsatz der Software durch Althammer & Kill überprüfen und per Testat bestätigen lassen. &

connextvivendi
Die Software für das Sozialwesen

unterlagen „gewährt“. Manche verstehen dies so, dass der Arzt den Einblick sozusagen Gnaden halber und nach seinem Ermessen bewilligen kann – oder eben auch nicht. Das trifft jedoch nicht zu. Vielmehr hat der Patient einen gesetzlichen Anspruch auf Einblick in die Behandlungsunterlagen, die ihn selbst betreffen. So regelt es ausdrücklich § 630g BGB.

Anspruch auf Kopien

Häufig wird es so sein, dass ein Patient die Unterlagen nicht versteht. Viele Begriffe sind nur Fachleuten klar. Und selbst ein Fachmann braucht Zeit, um den Inhalt von Unterlagen richtig zu interpretieren. Oft wollen Patienten deshalb Kopien ihrer Behandlungsakte. Auch dieser Anspruch ist gesetzlich inzwischen klar festgelegt (siehe § 630g Absatz 2 BGB: „Der Patient kann auch elektronische Abschriften von der Patientenakte verlangen.“).

Kostenpflicht für Kopien

Genauso klar ist allerdings auch geregelt, dass der Patient die Kosten hierfür tragen muss. Man sollte sie nicht unterschätzen. Denn selbstverständlich gehören dazu nicht nur die eigentlichen Kopierkosten, sondern auch die Kosten für das Personal, das Kopien anfertigt.

Glück hat ein Patient, dessen Patientenakte elektronisch geführt ist. Das Übertragen der Daten auf einen elektronischen Datenträger verursacht kaum irgendwelche Kosten.

Ansprüche der Erben und Angehörigen

Etwas schwierig wird es, wenn ein Patient verstorben ist. Relativ häufig wollen dann Angehörige wissen, wie es eigentlich zum Tod kam. Fragen dazu sind allerdings oft vergeblich. Das gilt sogar dann, wenn eine enge familiäre Beziehung besteht und beispielsweise die Ehefrau fragt, warum ihr Mann gestorben ist. Der Grund: Die ärztliche Schweigepflicht gilt auch nach dem Tod weiter, und der Gesetzgeber wollte sie nicht zu sehr aushöhlen.

Das Gesetz lässt deshalb den Anspruch auf Einsicht in die Behandlungsunterlagen nicht einfach pauschal auf die Erben oder auf nahe Angehörige übergehen. Vielmehr heißt es in § 630g Absatz 3 BGB, dass die Erben „zur Wahrnehmung vermögensrechtlicher Interessen“ Einblick in Behandlungsunterlagen nehmen dürfen.

Das praktisch wichtigste Beispiel hierfür: Die Lebensversicherung will nicht zahlen, weil sie die Umstände des Todes für unklar hält. Dann kann es für den Erben Gold wert sein, wenn er mithilfe der Behandlungsunterlagen nachweisen kann, dass die Versicherung sehr wohl zahlen muss.

Erst reden, dann zum Gesetz greifen

Insgesamt hat der Gesetzgeber die Rechte der Patienten in den letzten Jahren gestärkt. Grenzen haben diese Rechte allerdings nach wie vor. Suchen Sie deshalb immer zunächst das Gespräch mit dem Arzt, der Sie behandelt hat. Greifen Sie erst dann zum Gesetz, wenn sonst wirklich kein vernünftiges Ergebnis zu erzielen ist. &

5
Datenschutz *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 5/2016
ALTHAMMER & KILL

Der Kindergeburtstag auf Facebook

Welche Regeln gelten eigentlich, wenn man Fotos von einem Kindergeburtstag auf Facebook stellen will? Ärger ist in solchen Fällen häufiger als man denkt. Kurzes Nachdenken vorher verhindert Schwierigkeiten nachher!

Der Kindergeburtstag war eine schöne Sache. Die Kinder amüsierten sich prima. Und manche Eltern waren froh, ihren Nachwuchs einfach einmal für einen Nachmittag bei lieben Nachbarn abgeben zu können. Es entstanden dabei wirklich schöne Fotos. Daran wollte der Vater des Geburtstagskinds auch andere teilhaben lassen. Deshalb wählte er zehn besonders schöne Fotos aus und stellte sie auf die eigene Facebook-Seite.

Kinderfotos auf Facebook – gute Idee oder nicht?

Ob das eine gute Idee war, darüber gingen die Meinungen schnell auseinander. Probleme gab es vor allem mit den Eltern eines Kindes, das beim Geburtstag dabei war und das gleich auf mehreren Fotos zu sehen war. Dessen Eltern leben nämlich getrennt. Der Vater fand das mit den Fotos auf Facebook ganz gut. Die Mutter hielt dagegen überhaupt nichts davon.

Klare gesetzliche Regelungen

Solche Fälle muss man sich nicht ausdenken. Wenn man sich etwas umhört, wird man rasch fündig. Und schon stellt sich die Frage, was in solchen Fällen eigentlich zu beachten ist. So sehr es manchen wundert: Es gibt dafür klare gesetzliche Regeln. Sie stehen in einem Gesetz, das schon über 100 Jahre alt ist. Es wird meistens mit seiner Abkürzung KUG erwähnt. Sein vollständiger Name „Kunsturheberrechtsgesetz" ist zum einen recht sperrig. Zum anderen führt er auch in die Irre. Die Regelungen in diesem Gesetz haben nämlich nichts mit dem Urheberrecht zu tun und auch nichts mit der Kunst. Vielmehr geht es um das, was die Juristen „Recht am eigenen Bild" nennen. Das Urheberrecht ist dagegen inzwischen in einem anderen Gesetz geregelt.

Einwilligung nötig – bei Minderjährigen von den Eltern

Beim Recht am eigenen Bild geht es um die Frage, ob es jemand dulden muss, dass Bilder von seiner Person verbreitet werden. Die Grundregel hierfür lautet klar: Nein, das muss er nicht. Wenn ich Bilder von jemandem verbreiten will, brauche ich seine Einwilligung dazu.

Das gilt natürlich auch für Kinder. Einzige Besonderheit: In diesem Fall kann nicht das Kind selbst einwilligen. Vielmehr brauche ich die Einwilligung der Eltern.

Besonderheiten eines Kindergeburtstags

Damit ist man sofort wieder beim Kindergeburtstag, von dem Fotos auf Facebook verbreitet werden. Daran ist Folgendes rechtlich wichtig:

– Fotos auf Facebook sind normalerweise öffentlich zugänglich. Das gilt vor allem dann, wenn der Zugriff nicht auf bestimmte Personen beschränkt ist.
– Aber auch dann, wenn eine solche Beschränkung auf bestimmte Personen vorgenommen wird, ändert das nichts daran, dass die Bilder jedenfalls gegenüber diesen Personen verbreitet werden.
– Man kann es also drehen und wenden, wie man will: Bilder von Personen darf man normalerweise nur dann auf Facebook einstellen, wenn man die Einwilligung dieser Personen hat.
– Bei Kindern ist es Sache der Eltern, ob sie einwilligen oder nicht.
– Das ist kein Problem, solange sich die Eltern einig sind. Was aber ist, wenn ein Elternteil Ja sagt und ein Elternteil Nein? Wenn beide Eltern anwesend sind und sich vor Ort so verhalten, ist ein Einstellen der Bilder auf Facebook ausgeschlossen.
– Und wie sieht es aus, wenn nur ein Elternteil anwesend ist? Muss man dann den anderen anrufen und ihn ebenfalls fragen? Nach Auffassung der meisten Juristen gehört eine solche Einwilligung zu den alltäglichen Dingen, die auch ein Elternteil für sich allein erledigen kann. Aber hier muss man ein bisschen vorsichtig sein. Ginge es beispielsweise um Fotos für Werbezwecke, sähe das schon wieder anders aus. Denn das ist dann keine banale Angelegenheit mehr.

Das immer zulässige „Gruppenfoto" – ein rechtlicher Mythos

Häufig hört man, dass es kein Problem sei, wenn man Bilder einer Gruppe veröffentliche. Und manche wollen sogar wissen, das gelte vor allem dann, wenn die Gruppe aus sieben oder mehr Personen besteht. Manchmal wird sogar behauptet, diese Zahl 7 stünde sogar im Gesetz.

Nichts davon ist wahr. Es handelt sich vielmehr um ein Beispiel für rechtliche Märchen. Zwar gibt es im KUG eine Regelung für Fotos von Demonstrationen, Umzügen und ähnlichen Ereignissen. Es ist klar, dass man davon nie Bilder veröffentlichen könnte, wenn man die Einwilligung aller beteiligten Personen bräuchte.

Deshalb fordert das Gesetz für diese speziellen Fälle keine Einwilligung. Man kann sie fotografieren und diese Fotos auch verbreiten und veröffentlichen. Kindergeburtstage gehören jedoch sicher nicht in diese Kategorie. &

Damit der Online-Kalender nicht zum Datenleck wird

Ein digitaler Kalender, der über das Internet gepflegt wird, ist wirklich praktisch. Leider ist er auch wirklich gefährlich, wenn der Datenschutz nicht stimmt.

Stellen Sie sich vor, Sie sind beruflich unterwegs und bekommen einen Anruf. Es ist der Leiter einer anderen Abteilung, der Sie zu einem Projekttreffen einlädt. Da sind Sie gern dabei, Sie sagen zu. Kurze Zeit später ruft jemand aus Ihrer Familie an und berichtet von einer Einladung der Nachbarn. Ob Sie dann Zeit haben, lautet die Frage. Nach Ihrer Erinnerung schon, Sie sagen wieder zu.

Zurück im Büro schauen Sie in Ihren Kalender. Sie ahnen es schon: Sowohl bei dem Projekttreffen als auch bei der Einladung der Nachbarn haben Sie bestehende Termine übersehen. Solche Terminüberschneidungen sind mehr als ärgerlich.

Bei Ihnen kommt das nicht vor, da Sie einen Online-Kalender nutzen, auf den Sie über das Internet auch unterwegs Zugriff haben? Dann haben Sie vielleicht keine Terminüberschneidungen. Dafür aber möglicherweise ein Datenleck.

Vertrauliche Daten in Kalendern sind oftmals ungeschützt

Bekanntlich steht es um die Verschlüsselung von E-Mails nicht gut (siehe auch Seite 1). Vertrauliche Daten wer-

den unverschlüsselt über das Internet übertragen. Was leider übersehen wird: Das ist bei so manchem Online-Kalender nicht anders. In den digitalen Kalendern stehen vertrauliche Termine und Kontakte. Doch verschlüsselt werden die Inhalte der Kalender kaum.

Durch den möglichen Online-Zugriff auf den Kalender müssen Sie mit Datenrisiken aus dem Internet rechnen. Dazu gehören gefälschte Termineinladungen, die nur darauf abzielen, an Ihr Passwort für den Online-Kalender zu gelangen. Solche Angriffe beginnen mit einer scheinbaren Termin-Einladung, enthalten einen manipulierten Link auf den Online-Termin und fangen dann die Zugangsdaten zu Ihrem Online-Kalender ab. Phishing-Angriffe und Passwortdiebstahl gibt es eben leider auch bei Kalendern.

Terminkalender: voll von Terminen und Risiken

Viele der Funktionen von Online-Kalendern, die sehr praktisch sind, können zur Gefahr für Ihre Daten werden, wenn Sie nicht genug für den Datenschutz tun.

Online-Kalender bieten Freigabefunktionen für einzelne Termine, für alle Termine bis hin zur Veröffentlichung ganzer Kalender im Web. Vorsicht: Sie könnten versehentlich Termine mit personenbezogenen Daten zu Suchmaschinen-Futter machen, also öffentlich ins Netz stellen. Am besten tragen Sie nur Termine in einem Online-Kalender ein, die Sie auch ans Schwarze Brett hängen würden. Andernfalls ist zusätzlicher Schutz erforderlich.

Bei dem Import aus anderen Kalender-Programmen sollten Sie ebenfalls vorsichtig sein. Prüfen Sie nach dem Import genau, welchen Status die importierten Termine haben, zum Beispiel öffentlich oder privat. Funktionen von Kalendern wie Dateianhang machen klar, dass digitale Kalender in Wirklichkeit Kommunikationsanwendungen sind. Damit ist auch klar, dass Dateien, die mit Terminen übertragen werden, genauso schadhaft sein können wie der Anhang einer E-Mail.

Online-Kalender: Kennen Sie die Risiken? Machen Sie den Test!

Frage: Um Online-Kalender zu schützen, reicht ein starkes Passwort. Stimmt das?

a. Ja, dank Passwortschutz kann kein Unbefugter meine Termine lesen.
b. Nein, Datendiebe versuchen, auch die Passwörter für Online-Kalender zu stehlen.

Lösung: Die Antwort b. ist richtig. Auch bei Online-Kalendern gibt es Phishing-Attacken. Schützen Sie daher vertrauliche Inhalte genau wie bei E-Mail zusätzlich. Achten Sie bei der Wahl des Online-Kalenders auf eine Verschlüsselung.

Frage: Der klassische Kalender ist sicherer als ein digitaler. Stimmen Sie dem zu?

a. Nein, ohne besonderen Schutz können natürlich auch Kalender in Papierform eingesehen werden. Jeder Kalender braucht einen Zugangsschutz.
b. Ja, denn mit dem Internet kommen neue Risiken für vertrauliche Termine hinzu. Datendiebe können unerkannt über das Internet die zu schützenden Termine lesen und sogar verändern oder löschen.

Lösung: Die Antwort a. ist richtig, gleichzeitig aber auch die Antwort b. Vertrauliche Termine müssen grundsätzlich geschützt werden, bei Kalendern in Papierform und bei digitalen Kalendern. Durch das Internet können auch Unbefugte Zugriff erlangen, die nicht an einen Kalender in Papierform kommen würden, wenn dieser auf dem Schreibtisch liegt. Doch auch die Kalender auf dem Schreibtisch müssen besser geschützt werden. Räumen Sie daher bitte Ihren Kalender weg, wenn Sie den Schreibtisch verlassen.

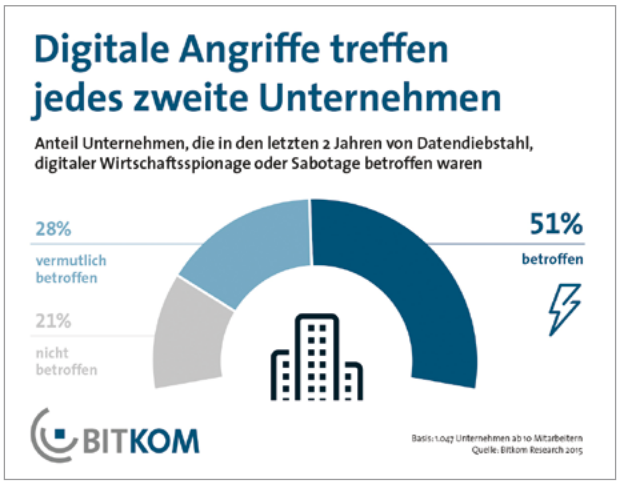
Tipps: Datenschutz bei Online-Kalendern

- Verzichten Sie auf generelle Freigaben und definieren Sie lieber die Freigabe konkret bei Einzelterminen!
- Prüfen Sie die angehängten Dateien zu Terminen auf Malware!
- Denken Sie bei Einladungen zu Terminen an mögliches Phishing!
- Wählen Sie Passwörter der digitalen Kalender ausreichend stark!
- Überprüfen Sie Termin-Importe auf falsche Freigaben!
- Denken Sie auch bei digitalen Kalendern an die Datensparsamkeit! &

Sicherheitsmaßnahmen wirksam überprüfen

IT-Sicherheitsexperten von Althammer & Kill testen die Anfälligkeit Ihrer IT-Systeme

Fast täglich wird von Hacking-Attacken auf Unternehmen, Behörden und Organisationen berichtet. Nach einer aktuellen BITKOM-Studie waren bereits 51% der Unternehmen in Deutschland von Datendiebstahl, digitaler Wirtschaftsspionage oder Sabotage betroffen, weitere 28% vermuten, dass es Angriffe oder Angriffsversuche gegeben hat.

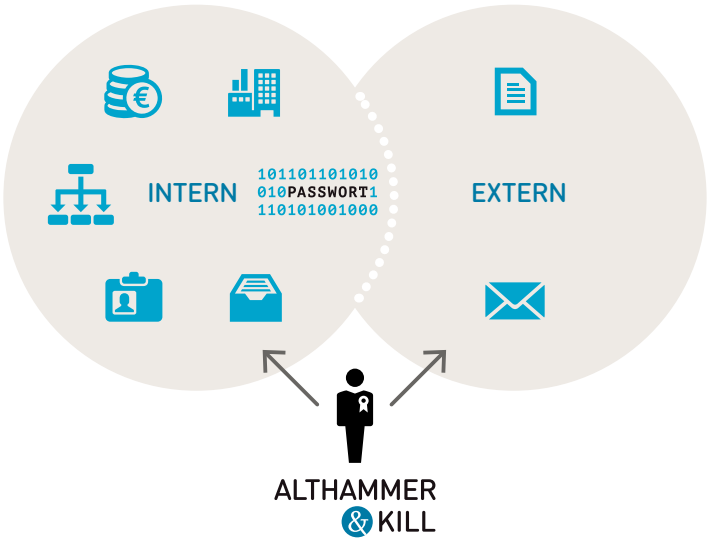


Mit zunehmender Komplexität und Vernetzung der IT-Systeme fällt es schwer, alle Schutzsysteme und Software-Komponenten auf einem aktuellen Stand zu halten. Die Zahl der Lücken steigt weiterhin laut der BSI-Schwachstellenampel. Für die „Kreativen" (Hacker) gibt es eine große Zahl von Angriffsvektoren und möglichen Einfallstoren. Systemmanagement, Zufall und Glück entscheiden, wer in welchem Umfang hiervon betroffen ist.

Im Rahmen sogenannter „Penetrationstests" bieten wir an, die Wirksamkeit der heutigen Maßnahmen zur Informationssicherheit durch einen teilautomatisierten Test möglicher Angriffsszenarien zu überprüfen. Dabei lassen sich u. a. die folgenden Szenarien untersuchen:

Szenario „Internet-Angriff"

Es wird ein Angriff von außen auf öffentlich über das Internet zugängliche Systeme simuliert, z. B. Webserver, E-Mail-Server und weitere Angebote. Die erreichbaren Dienste dieser Systeme werden auf Schwachstellen analysiert.



Szenario „Netzwerk-Angriff"

In diesem Szenario hat der simulierte Angreifer Zugang zum internen Netzwerk. Dies entspricht zum Beispiel der Situation, dass ein von Mitarbeitern verwendetes Gerät kompromittiert wurde und nun als Sprungbrett für weitere Angriffe genutzt wird, oder dass jemand unbefugter Weise ein solches Gerät in Ihr Netzwerk eingebracht hat. In diesem Szenario hat der Angreifer jedoch zu Beginn der Simulation kein Benutzerkonto im Netzwerk.

Szenario „Arbeitsplatz-Angriff"

Hier wird ein Angriff simuliert, wie er von einem „Insider" ausgehen könnte. Dazu benötigen wir einen von Ihnen bereitgestellten Arbeitsplatz-PC oder Laptop in der Standard-Konfiguration. Erforderlich ist ein „normal" privilegiertes Benutzerkonto mit Zugriffsrechten im Netzwerk. Wir versuchen, auf Basis von Lücken in der Systemkonfiguration an vertrauliche Daten und erweiterte Zugriffsrechte zu erlangen.

Bei Interesse beraten wir gern und unterbreiten ein unverbindliches Angebot. &

E-Mail und Internet im Unternehmen: Sicher betreiben, rechtskonform gestalten.

Die Nutzung von E-Mails und Internet-Diensten sind aus dem Unternehmensalltag nicht mehr wegzudenken. Jüngste Sicherheitsvorfälle wie der gelungene Hacking-Angriff auf den Bundestag machen jedoch deutlich, welche Gefahren im Netz lauern. Wir zeigen typische Risiken auf und stellen unsere modulare IT-Security-Plattform für den Unternehmenseinsatz vor.

Die Funktionsweise von Viren und Trojanern ist vielen bekannt. Fast jeder PC ist mit einem Virenscanner ausgestattet. Doch die Inhalte von Websites stellen nach regelmäßigen Umfragen die höchste Bedrohung für IT-Systeme dar.

Über infizierte Webserver und Sicherheitslücken in Browsern schleusen Angreifer Schadcode in unternehmensinterne IT-Infrastrukturen ein oder spähen Zugangsdaten und persönliche Informationen aus.

Webfilter: Der „Virenscanner" für Webseiten

Meist arbeiten diese Schadprogramme im Verborgenen um möglichst unentdeckt weitere IT-Systeme kompromittieren zu können. Die in den meisten Unternehmen eingesetzten Firewall- und Antiviren-Lösungen sind zwar in jedem Fall notwendig, bieten aber häufig keinen ausreichenden Schutz gegen diese neuartigen Bedrohungen.

Unser Webfilter schützt vor solchen Angriffen durch Analyse und Sperre der betroffenen Webseiten. Dabei lassen sich auch interne Vorschriften und rechtlichen Vorgaben umsetzen, z. B. die Sperrung unangemessener oder rechtswidriger Inhalte.

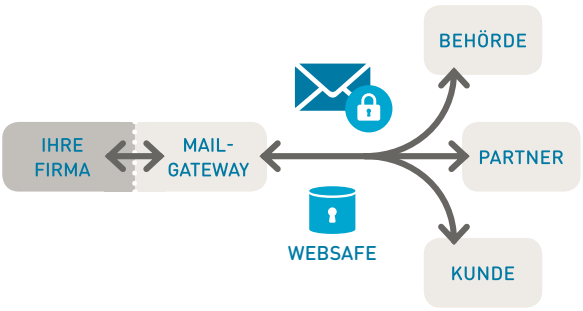
E-Mail-Verschlüsselung: Vertrauliches schützen

E-Mail stellt heute den zentralen elektronischen Kommunikationskanal und somit einen hochkritischen Dienst für alle Unternehmen dar. Wesentliche Eigenschaften von E-Mail sind Schnelligkeit und Einfachheit der Übertragung zum Empfänger sowie die Schriftform. Letztere macht E-Mail zu einem nachhaltigen Medium.

Geschäftliche E-Mails enthalten oftmals interne, persönliche oder andere sensible Inhalte, die besonders vor Ausspähung geschützt werden müssen. Vor allem die Enthüllungen rund um die NSA-Abhörpraktiken haben gezeigt, dass der Inhalt von E-Mails ohne weitere Vorkehrungen nicht sicher ist.

Im Prinzip gleicht dieser dem Verschicken von Postkarten. Allerdings enthalten Postkarten meist keine hochvertraulichen Informationen und werden erst recht nicht für geschäftliche Zwecke verwendet. Eine starke Verschlüsselungslösung schafft hier Abhilfe. Zwar existieren seit Anfang der 1990er Jahre robuste und bewährte Standards zur Absicherung der E-Mail-Kommunikation. Der Einsatz dieser Verschlüsselungstechnologien ist jedoch schwierig (Komfort vs. Sicherheit).

Wir bieten eine zentrale Lösung an, die vollautomatisch und transparent im Hintergrund bei Bedarf ein- und ausgehende E-Mails nach den gängigen Standards (S/MIME, PGP) verschlüsselt bzw. entschlüsselt. Das entlastet Ihre Mitarbeiter, minimiert den Administrationsaufwand und trägt zur rechtskonformen Übertragung von Information bei.



E-Mail-Archivierung: Nicht nur für das Finanzamt

Für klassische Kommunikation in Schriftform oder Fax haben Unternehmen klare Regeln, wie diese geleitet, erfasst und abgelegt werden. Schriftstücke werden z. B. chronologisch oder vorgangsbasiert in Ordnern abgelegt und archiviert. Die Ablage als Papierdokument ermöglicht den Nachweis, dass es sich um ein unverändertes Original handelt, welches

auch als Beweis vor Gericht verwendet werden kann.

Per E-Mail ausgetauschte Informationen können noch nach langer Zeit wieder eingesehen werden, wenn die E-Mail dann noch gespeichert ist und man die entsprechende E-Mail auch findet. Das Bundesministerium für Finanzen hat in den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD, ehemals GDPdU), die einschlägigen Rechtsnormen zur revisionssicheren Ablage über längere Zeiträume konkretisiert. Demnach reicht eine einfache Ablage im Dateisystem nicht mehr aus. Eine E-Mail samt Anhang muss im Originalzustand schnell verfügbar sein und jede Änderung muss protokoliert werden.

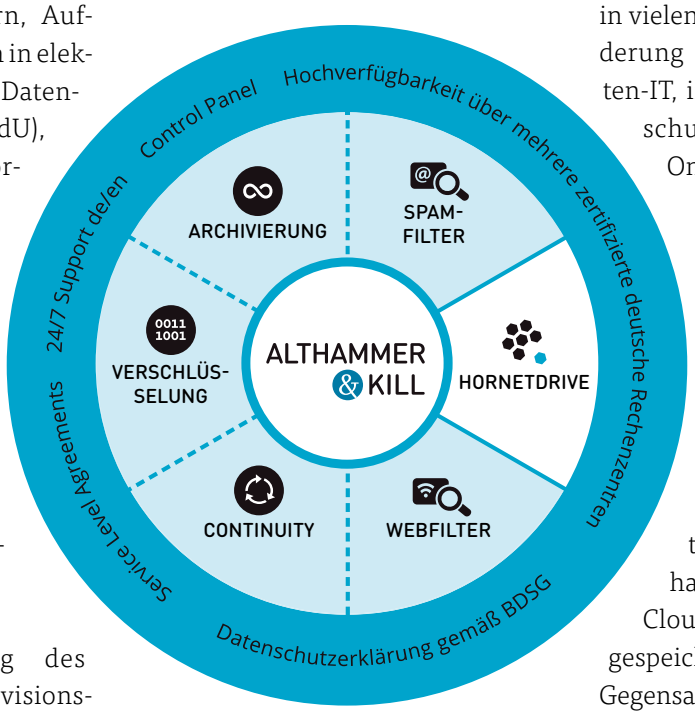
Eine sinnvolle Kopplung des E-Mail-Systems mit einer revisionssicheren Archiv-Lösung ist nicht nur zwingend vorgeschrieben, sie sollte auch möglichst transparent und benutzerfreundlich konzipiert werden. Unsere Lösung lässt sich leicht in bestehende Umgebungen integrieren und kostengünstig betreiben.

E-Mail-Continuity-Service: Notfallschutz für Ihren E-Mail-Server

Es ist der Albtraum eines jeden IT-Verantwortlichen: Das E-Mail-System fällt plötzlich aus, Mails können weder empfangen noch verschickt werden. Eine brenzlige Situation für jedes Unternehmen.

Unser E-Mail-Continuity-Service ist der „doppelte Boden“ für Ihre E-Mail-Infrastruktur. Als zuverlässiges Standby-System kann unser System im Notfall einspringen, so dass keine E-Mails verloren gehen und die Mitarbeiter weiterhin Nachrichten versenden und empfangen können.

Das Konzept erlaubt eine sekundenschnelle Umschaltung für den Fall,



dass interne E-Mail-Server wie z. B. Microsoft Exchange nicht zur Verfügung stehen. Damit wird selbst während des Ausfalls des eigenen Mailservers der Zugriff auf gesicherte E-Mails ermöglicht.

Hornetdrive: Auch unterwegs alles dabei

Für größere Dateien stellt die E-Mail-Kommunikation keine geeignete Lösung dar. Wuchtige Datei-Anhänge sind oft nicht zulässig, die Übertragung ist sperrig und der Zugriff unübersichtlich. Dennoch greifen viele Mitarbeiter heute von unterwegs, einem Partnerstandort oder von Zuhause auf geschäftliche Daten zu. Oftmals müssen diese zusätzlich mit Kollegen oder Geschäftspartnern ausgetauscht werden.

Ein weltweiter Zugriff – unabhängig von dem eingesetzten Gerät oder Betriebssystem – stellt viele Organisationen vor eine große Herausforderung. Gerade diese Problematik führt in vielen Unternehmen auch zur Förderung einer sogenannten Schatten-IT, in der Mitarbeiter auf datenschutzrechtlich fragwürdige Online-Dienste ausweichen.

Unsere Lösung Hornetdrive ersetzt das Netzlaufwerk und hält lokale Ordner synchron mit anderen Benutzern, die ebenfalls Zugriff auf das Verzeichnis haben. Jede Änderung einer Datei wird verschlüsselt an zentraler Stelle gesichert. Dabei hat das Rechenzentrum „in der Cloud“ keine Möglichkeit, an die gespeicherten Daten zu gelangen. Im Gegensatz zu Dropbox, OneDrive & Co. erfolgt die Speicherung ausschließlich in Deutschland und unter Einhaltung aller geltenden Datenschutzgesetze.

Unser Angebot

Wir kennen die o. g. Szenarien nur allzu gut und möchten Ihnen unsere unterstützenden Lösungen für die geschilderten Problemstellungen gern näher vorstellen. Bei Interesse zeigen wir Ihnen die Funktionen live im Rahmen eines Webinars oder auch gerne bei einem persönlichen Besuch in Ihrem Unternehmen. &

Termine

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

26.10.2016 – 27.10.2016, Nürnberg
Messe ConSozial 2016
Wir freuen uns auf Ihren Besuch!

26.10.2016, Nürnberg
Vortrag Update Datenschutz, Messe ConSozial 2016
2018 kommt die EU-Datenschutz-Grundverordnung! Wie Sie Ihre Einrichtung schon jetzt darauf vorbereiten können/sollten.

27.10.2016, Stuttgart
Deutsche Bank Kirchenforum Stuttgart
Sicherheit ist relativ – Sicherheit neu denken

09.11.2016 – 10.11.2016, Königstein
Sinfonie Anwendertagung 2016
Treffen Sie uns bei sinfonie in Königstein!

15.11.2016, Bielefeld
FHdD Webinar – Datenschutz im Gesundheits- und Sozialwesen
Kein Tag vergeht, an dem nicht über Datenschutz und IT-Sicherheitspannen in der Presse berichtet wird.

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

News

Aus unserem aktuellen Newsletter:

Kopierverbot für Ausweise
https://www.althammer-kill.de/news-detail/kopierverbot-fuer-ausweise.html

Kosten von Datenpannen und Pflicht zur Selbstanzeige
https://www.althammer-kill.de/news-detail/kosten-von-datenpannen-und-pflicht-zur-selbstanzeige.html

Keine Chance für CEO-Fraud, Ransomware und Co.
https://www.althammer-kill.de/news-detail/keine-chance-fuer-ceo-fraud-ransomware-und-co.html

Chrome warnt vor unverschlüsselten Websites
https://www.althammer-kill.de/news-detail/chrome-warnt-vor-unverschluesselten-websites.html

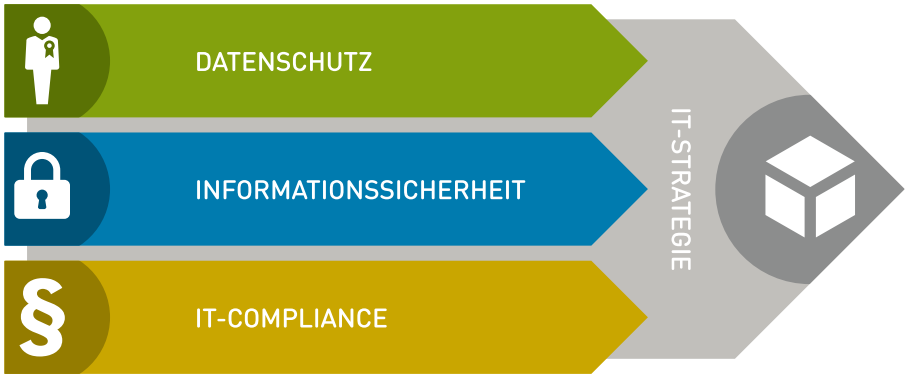
Häufigste Lüge im Netz – Bestätigung von AGBs
https://www.althammer-kill.de/news-detail/haeufigste-luege-im-netz-bestaetigung-von-agbs.html

Neue E-Mail Betrugsmasche
https://www.althammer-kill.de/news-detail/e-mail-betrugsmasche.html

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

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

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

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

Lars Begerow
Berater für IT-Strategie
Tel. +49 211 936748-40
lb@althammer-kill.de

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

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

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

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

Althammer & Kill GmbH & Co. KG

info@althammer-kill.de
www.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

Mitglied im: