**intimus consulting ist eine
Marke der
MARTIN YALE GROUP**
Bergheimer Straße 6-12
88677 Markdorf / Deutschland
www.intimusconsulting.com

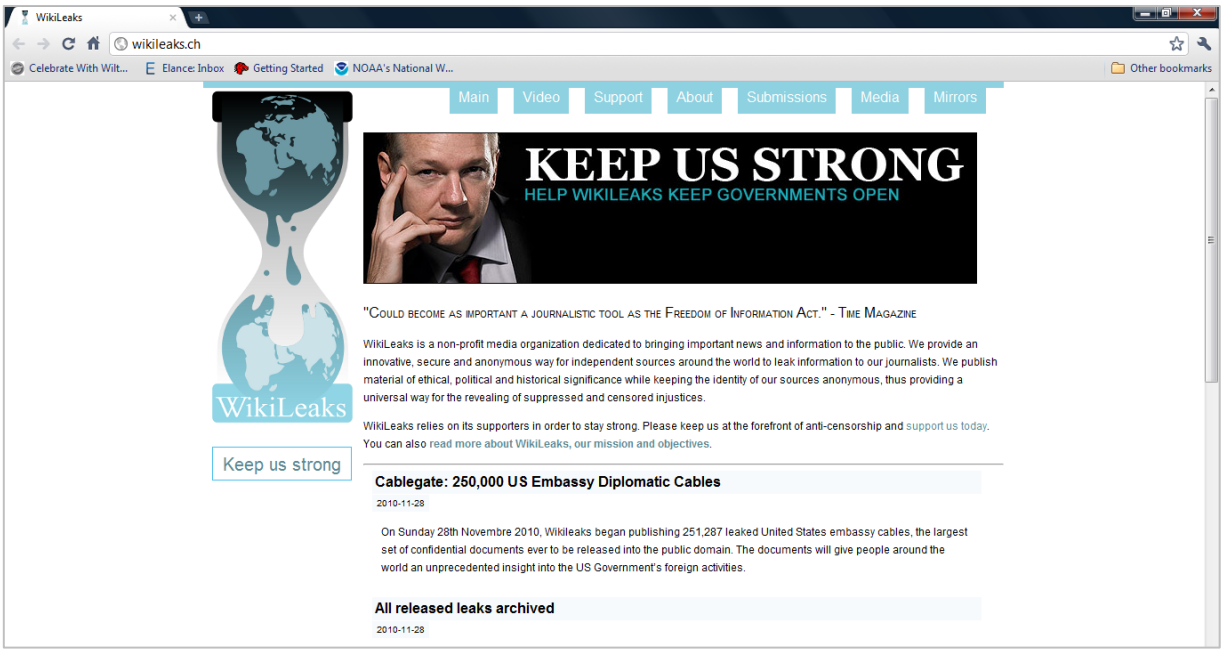
intimus®
SECURITY CONSULTING

Datenlecks verhindern: Informationssicherheit im Zeitalter von WikiLeaks

Whitepaper

intimus®
SECURITY CONSULTING

Datenlecks verhindern: Informationssicherheit im Zeitalter von WikiLeaks



Zusammenfassung

WikiLeaks wurde bekanntermaßen international berühmt (oder berüchtigt – je nach Standpunkt), als das Portal begann, geheime und vertrauliche Informationen, die ihm von Informanten aus Regierungskreisen zugespielt wurden, zu veröffentlichen.

WikiLeaks gewährte der gesamten Welt Einblicke in streng vertrauliche Daten des US-Militärs zu den Kriegen im Irak und in Afghanistan sowie in Tausende Seiten von Telegrammen und Depeschen des US-Außenministeriums.

Die US-Regierung und auch andere Regierungen rund um den Globus müssen sich der Tatsache stellen, dass im Zeitalter von WikiLeaks kein Staatsgeheimnis mehr sicher ist.

Was genau bedeutet dies nun für Ihr Unternehmen bzw. Ihre Behörde? Dieses Whitepaper erläutert einige der Lektionen, die Datenschutzbeauftragte in Unternehmen und staatlichen Behörden inzwischen aus dem Fall WikiLeaks gelernt haben sollten.

intimus®
SECURITY CONSULTING

Inhalt

Informationen verbreiten sich rasend schnell

Daniel Ellsberg
(Quelle: Wikimedia Commons)

Ernüchtert über die US-amerikanische Kriegsführung in Vietnam, entschloss sich Daniel Ellsberg, seines Zeichens US-Militäranalytiker, 1971 eine Reihe vertraulicher Dokumente des Militärs – die „Pentagon Papers“ – der New York Times und anderen Zeitungen zuzuspielen.

Diese Pentagon Papers repräsentieren die offizielle, aber damals geheime Chronologie der Entscheidungen und des zunehmenden Kriegsengagements der US-Regierung in Vietnam. Ihre Veröffentlichung leistete einen entscheidenden Beitrag, um die Stimmung im Lande zu kippen und die Friedensbewegung zu stärken. Daniel Ellsberg wurde in der Folge der Spionage angeklagt, später jedoch wegen Verfahrensfehlern freigelassen.

1971 war die Übermittlung einer solch großen Menge von vertraulichen Informationen eine komplexe und zeitaufwendige Angelegenheit. Daniel Ellsberg verbrachte Stunden damit, unbemerkt über 7.000 Seiten an Dokumenten zu fotokopieren, die er dann heimlich (und höchstpersönlich) seinen Kontakten bei verschiedenen Zeitungen und im US-Senat übergab. 1971 bedurfte es sowohl Zeit als auch gewisser Anstrengungen und physischen Platzes, um Tausende Seiten voller Informationen zu bearbeiten.

Heute jedoch, im Zeitalter von WikiLeaks, sind Informationen praktisch unsichtbar und verbreiten sich über Breitbandverbindungen und Cloud-Anwendungen. Statt Kopiergeräte und Stapel aus Papierdokumenten wie zu Ellsbergs Zeiten, nutzt WikiLeaks sichere Server und verschlüsselte E-Mails. Vertrauliche Informationen werden heute nicht mehr nur mit einigen auserwählten Zeitungsreportern geteilt, sondern ins Web gestellt und damit Millionen Menschen weltweit zugänglich gemacht.
Informationen, die Ihr Unternehmen bzw. Ihre Behörde als höchst vertraulich einstuft und die keinesfalls nach außen gelangen sollten, können einfacher als je zuvor verbreitet, kopiert und mit Anderen geteilt werden. Sind Ihre Protokolle und Maßnahmen zum Schutz Ihrer Informationen auf dem neuesten Stand und diesen Herausforderungen gewachsen?

Schutz vor der „am wenigsten vertrauenswürdigen Person“

Eine Kette ist nur so stark wie ihr schwächstes Glied. Und ebenso „sind Geheimnisse nur so sicher, wie dies die am wenigsten vertrauenswürdige eingeweihte Person zulässt“, so Bruce Schneier, Experte für Sicherheitstechnologien.[1] WikiLeaks hat es geschafft, vertrauliche Informationen der gesamten Welt zugänglich zu machen, und zwar schneller und effizienter als je zuvor – doch WikiLeaks gelangte an diese Informationen nicht dank irgendwelcher hochmoderner Technologien, sondern auf die altbewährte Weise: durch einen Informanten innerhalb der jeweiligen Behörde oder Organisation, der trotz Sicherheitsüberprüfung die Vorschriften verletzte und vertrauliche Daten nach außen gab.

Wer ist die „am wenigsten vertrauenswürdige Person“ in Ihrem Unternehmen bzw. Ihrer Behörde? Wo befindet sich das „schwächste Glied“ in den Protokollen und Maßnahmen zur Informationssicherung in Ihrem Unternehmen? Haben Sie entsprechende Kontrollen eingerichtet, um sicherzustellen, dass vertrauliche Informationen nur den ausgewählten Personen zugänglich sind, die diese Informationen tatsächlich benötigen? Klassifizieren Sie Ihre Informationen je nach Vertraulichkeitsstufe? Und ist gewährleistet, dass Daten abhängig von den potenziellen Folgen für das Unternehmen bei Bekanntwerden der jeweiligen Informationen entsprechend stark geschützt sind?

Jeder einzelne Aspekt in Ihrem Unternehmen bzw. Ihrer Behörde kann und sollte so gehandhabt werden, dass die Wahrscheinlichkeit eines Datenlecks minimiert wird. Dies betrifft Ihre alltäglichen Geschäftsvorgänge, Neueinstellungen, Schulungen, die Vergabe von Netzwerkpasswörtern, aber auch die Entscheidung darüber, ob Mitarbeiter eigene Speichermedien auf die Arbeit mitbringen dürfen, oder die Frage, wie Papierdokumente am Ende eines jeden Arbeitstages entsorgt werden sollen.

[1] Schneier, Bruce. http://www.schneier.com/blog/archives/2010/12/wikileaks_1.html

Achtung bei Anzeichen eines Datenlecks!

Das Verizon Security Blog kommentierte den Fall WikiLeaks und die verwendeten Methoden als nicht besonders neu oder überraschend: Bradley Manning, der US-Soldat, der als Hauptquelle für die meisten US-Militärinformationen in den Händen von WikiLeaks gilt, hatte bereits viele der klassischen Anzeichen eines potenziellen Sicherheitsrisikos gezeigt.

In den Worten des Bloggers von Verizon: „Die Handlungen Mannings weisen die typischen Merkmale auf, die wir immer wieder bei der Analyse von Datenlecks vorfinden: zu viele Rechte und Privilegien, kaum Rechenschaftspflicht, eine seltsame oder ungewöhnliche Arbeitsweise, eine Vorgeschichte mit fragwürdigem Verhalten, gewisse Ressentiments bzw. Frust, Verwendung eigener Speichermedien, Aufdeckung/Anzeige durch Außenstehende usw.“[2]

- **Zu viele Rechte und Privilegien:** Obwohl Bradley Manning erst 22 Jahre alt und ein Geheimdienstanalytiker niederen Rangs war (*Private First Class* – ein Gefreiter), hatte er Zugang zum SIPRNet, dem *Secret Internet Protocol Router Network*, das vom Verteidigungs- und Außenministerium der USA zur Übertragung vertraulicher Informationen genutzt wird.

- **Vorgeschichte mit fragwürdigem Verhalten:** Bradley Manning war 2009 für seinen Angriff auf einen Kameraden zurechtgewiesen und vom Rang eines Spezialisten auf den eines Gefreiten (*Private First Class*) degradiert worden. In mehreren Chat-Nachrichten, die später von der Washington Post veröffentlicht wurden, sagte Manning, dass ihm aufgrund „mangelnder Anpassungsfähigkeit“ die Entlassung aus der Armee drohe.[3]

  Wenn es in Ihrem Unternehmen bzw. Ihrer Behörde Personen gibt, die Zugang zu vertraulichen Daten besitzen, aber bereits Anzeichen von Verhaltensproblemen oder fehlendem Respekt für das Unternehmen gezeigt haben oder allgemein nicht den

[2] Baker, Wade. „William H. Murray editorial on WikiLeaks.“ 4. Jan. 2011. http://securityblog.verizonbusiness.com/2011/01/04/william-h-murray-editorial-on-wikileaks/
[3] Nakashima, Ellen. „Messages from alleged leaker Bradley Manning portray him as despondent soldier.“ http://www.washingtonpost.com/wp-dyn/content/article/2010/06/09/AR2010060906170.html

Ansprüchen und Standards des Unternehmens gerecht werden, dann wäre es möglicherweise besser (für beide Seiten), wenn die betroffenen Personen aus dem Unternehmen ausgegliedert werden, statt sie unter dem Risiko eines möglichen Verstoßes gegen die Informationssicherheit weiter zu beschäftigen.

Natürlich wird nicht jeder missmutige Mitarbeiter zwingend zum Datenleck. Allerdings besteht bei unzufriedenen Mitarbeitern ein höheres Risiko für Fehler, für Verstöße gegen Vorschriften oder für andere Versäumnisse, die unbeabsichtigt in Zuwiderhandlungen gegen den Datenschutz resultieren. Für die Informationssicherheit kann sich eine „sündige Nachlässigkeit" genauso verheerend auswirken wie ein „sündiges Vergehen".

- **Ressentiments bzw. Frust:** In dem Zeitraum vor seiner mutmaßlichen Preisgabe vertraulicher Dokumente deuteten mehrere Facebook-Einträge Mannings darauf hin, dass er über sein Leben frustriert war, sich auf Arbeit isoliert fühlte, dem Militär wütend gegenüberstand und dass ihn seine schlechten Karriereaussichten deprimierten.[4] Missgestimmte, unzufriedene Mitarbeiter, die mit ihrem Leben oder ihrer Karriere nicht glücklich sind, stellen oftmals das größte Risiko für die Informationssicherheit dar – und diese Warnhinweise werden sogar oft durch Mitarbeiter oder Vorgesetzte bemerkt. Gibt es in Ihrem Unternehmen Maßnahmen, mit denen sich verdächtige Verhaltensweisen überwachen lassen, die ein Risiko für die Informationssicherheit darstellen?

- **Verwendung eigener Speichermedien/-geräte:** Manning brachte eigene, mit Musik bespielte CD-RWs mit an seinen Arbeitsplatz, löschte die CDs und brannte dann die heruntergeladenen vertraulichen Dokumente darauf. Manning beschrieb die Maßnahmen zur Informationssicherung des US-Militärs als „anfällige… auf gewisse Weise bemitleidenswerte… schwache Server, schwache Protokolle, schwache physische Sicherheitsmaßnahmen, schwache Gegenspionage, schwache

[4] Heidi Blake, John Bingham und Gordon Rayner, The Telegraph, 30. Juli 2010, online veröffentlicht unter http://www.telegraph.co.uk/news/newstopics/politics/defence/7918632/Bradley-Manning-suspected-source-of-Wikileaks-documents-raged-on-his-Facebook-page.html [abgerufen am 27. Jan. 2011]

Signalanalyse… die reinste Verkettung von Problemen."[5] Unternehmen müssen strenge Richtlinien in Bezug auf die Nutzung privater Speichermedien und -geräte durch Mitarbeiter aufstellen. Egal, ob Sie nun alle persönlichen Speichermedien verbannen oder Vorschriften mit gewissen Ausnahmeregelungen verhängen wollen – es muss auf jeden Fall eine Richtlinie existieren, welche die Erwartungen dem Personal gegenüber klar beschreibt und dem Unternehmen ein entsprechendes Maß an Sicherheit bietet.

- **Aufdeckung/Anzeige durch Außenstehende:** Bradley Manning wurde nicht durch den Geheimdienst des US-Militärs oder durch die CIA gefasst, sondern den Behörden durch Adrian Lamo gemeldet, seines Zeichens ein ehemaliger Hacker, den Manning kontaktiert hatte, nachdem dieser im Magazin *Wired* porträtiert worden war. Viele Unternehmen bemerken erst, dass die Sicherheit ihrer Informationen kompromittiert wurde, wenn sie über die Medien davon erfahren. Gibt es in Ihrem Unternehmen bzw. Ihrer Behörde ein „Frühwarnsystem" für potenzielle Datenlecks? Wenn vertrauliche Informationen Ihres Unternehmens nach außen gelangen – wie würden Sie davon erfahren?

Rückblickend scheint es unglaublich, dass so ein junger Soldat mit keineswegs makellosem Führungszeugnis derart einfach und unbemerkt auf Tausende Seiten höchst vertraulicher Dokumente zugreifen konnte. Daniel Ellsberg war ein hochrangiger Militäranalytiker mit besonderen Zugriffsprivilegien für geheime Regierungsakten und es kostete ihn viele Stunden, die 7.000 Seiten zu kopieren und daraus die Pentagon Papers zu erstellen. Bradley Manning hingegen spazierte ungehindert mit einigen wenigen CDs aus seinem Büro und verursachte damit das größte Datenleck in der Geschichte des US-Militärs.

Hinterher ist man natürlich immer klüger, jedoch sollte jedes Unternehmen eine wichtige Lektion aus dem Fall WikiLeaks gelernt haben: Unternehmensrichtlinien sind zu überprüfen und es muss sichergestellt werden, dass nicht sämtliche höchst vertraulichen Informationen jedem Mitarbeiter des Unternehmens zugänglich sind. Je mehr Personen Zugang zu Informationen haben, umso höher ist die Wahrscheinlichkeit, dass die Informationen nach außen gelangen –

[5] Wikipedia, online veröffentlicht unter http://en.wikipedia.org/wiki/Bradley_Manning [abgerufen am 27. Jan. 2011]

genauso, wie jede Kette nur so stark ist wie ihr schwächstes Glied, sind Geheimnisse auch nur so sicher, wie dies die „am wenigsten vertrauenswürdige eingeweihte Person“ zulässt.

Die enormen Kosten eines Datenlecks – oder eines Gerüchts darüber

Im November 2010 verkündete WikiLeaks, dass man sich im Besitz von 5 GB an Daten von der Festplatte eines leitenden Angestellten der Bank of America befinde – und diese Informationen veröffentlichen werde. Obwohl zu diesem Zeitpunkt noch keine der Daten preisgegeben worden waren, fielen die Aktien der Bank of America aufgrund dieser Meldung um 3 %.[6] Dieselben „altmodischen“ Datenlecks, durch die WikiLeaks Regierungsgeheimnisse enthüllt hatte, dienen nun dazu, vertrauliche Informationen privatwirtschaftlicher Unternehmen zu kompromittieren. Dazu bedarf es lediglich einer einzelnen Festplatte, die entweder ungeplant in die falschen Hände fällt oder den Enthüllern von einem einzelnen unzufriedenen Mitarbeiter zugespielt wird.

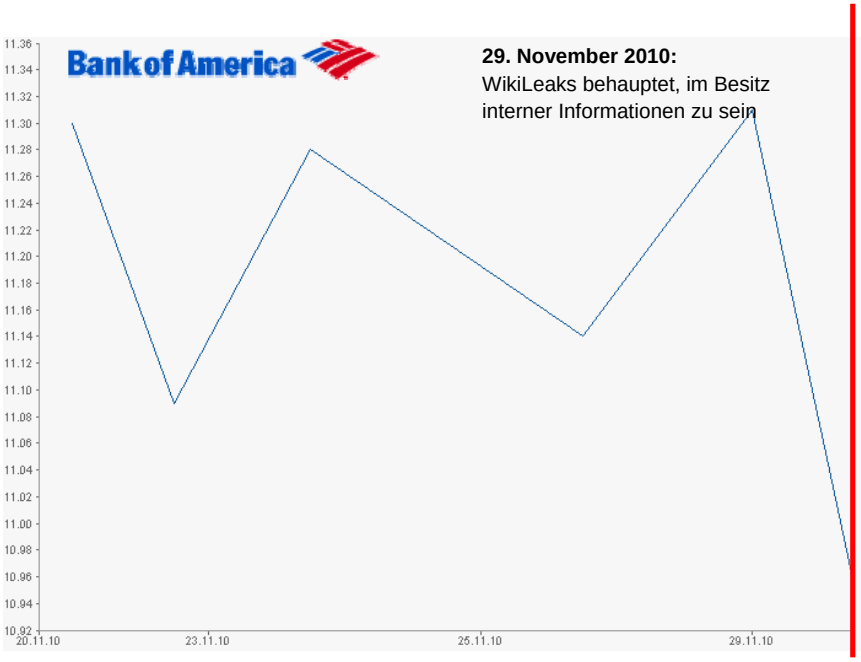


Abbildung 1: erstellt unter www.finanzen.net

[6] John Carney, CNBC.com, „Bank of America’s Risky WikiLeaks Strategy,” 2. Dez. 2010, online veröffentlicht unter http://www.cnbc.com/id/40471184/Bank_of_America_s_Risky_WikiLeaks_Strategy [abgerufen am 27. Jan. 2011]

Bei der Informationssicherheit geht es nicht nur um Technologien

Obwohl moderne Technologien oder besser durchdachte Sicherheitssysteme die nicht autorisierte Preisgabe vertraulicher Informationen an WikiLeaks durch Bradley Manning möglicherweise hätten verhindern können, ist der technologische Aspekt allein nicht die Lösung für das Problem. Wie Christopher Porter im Verizon Security Blog schreibt: „Sicherheitstechnologien sind kein Allheilmittel. Das Ganze ist ein viel komplexerer Prozess und die nötige Technologie ist nur ein Teil des Puzzles. […] Bei der Mehrheit der Vorfälle existieren bereits entsprechende Technologien und sogar Anzeichen für Verstöße gegen die Informationssicherheit – es sucht nur niemand danach."[7]

Bei den meisten Hilfsmitteln, die Unternehmen zum besseren Schutz ihrer Informationen einsetzen, geht es weniger um „Technologien", sondern um Vorschriften, Kontrollmechanismen und Zugriffsbeschränkungen für vertrauliche Informationen. Die Autoren des Verizon Security Blog hoffen für 2011 auf „eine Bewegung hin zur Übernahme durchaus bekannter, aber bisher kaum beachteter Konzepte wie das der „geringstmöglichen Privilegien" (*Least Privilege*), der Kenntnisnotwendigkeit (*Need to Know*) und der Rechenschaftspflicht (*Accountability*)."[8]

- **Geringstmögliche Privilegien:** Individuelle Nutzer sollten nur über die Zugriffsrechte verfügen, die zur Ausübung ihrer Aufgaben wirklich nötig sind. Ein 22-jähriger Gefreiter hatte Zugang zu Hunderttausenden von verschlüsselten Depeschen des US-Außenministeriums. Rückblickend kann dies nur als äußerst peinliches Versehen bezeichnet werden – warum hatten so viele Personen Zugang zu diesen Akten, die keinerlei Bedeutung oder Notwendigkeit für ihre Aufgaben haben? Gibt es auch in Ihrem Unternehmen „Versehen" wie dieses, wodurch vertrauliche Informationen Personen zugänglich werden, die diese Informationen überhaupt nicht kennen müssten?

[7] Christopher Porter, „Security Can Not Be Addressed by Technology Alone," 6. Dez. 2010, online veröffentlicht unter http://securityblog.verizonbusiness.com/2010/12/06/security-can-not-be-addressed-by-technology-alone/ [abgerufen am 15. Jan. 2011]

[8] Wade Baker, „William H. Murray editorial on WikiLeaks," 4. Jan. 2011, online veröffentlicht unter http://securityblog.verizonbusiness.com/2011/01/04/william-h-murray-editorial-on-wikileaks/ [abgerufen am 15. Jan. 2011]

- **Kenntnisnotwendigkeit:** Vertrauliche Informationen sollten nur den Mitarbeitern innerhalb des Unternehmens gegenüber preisgegeben werden, die eine spezifische Notwendigkeit zur Kenntnis dieser Informationen vorweisen können. Das Konzept der Kenntnisnotwendigkeit verhindert, dass beliebige Mitarbeiter vertrauliche Informationen völlig ungehindert „durchstöbern“ können (so wie dies Bradley Manning angeblich mit den Tausenden Depeschen des US-Außenministeriums tat). Wie stark achtet Ihr Unternehmen darauf, dass vertrauliche Informationen nur denjenigen individuellen Mitarbeitern zugänglich sind, die diese wirklich benötigen?

- **Rechenschaftspflicht:** Auf jeder Ebene des Unternehmens muss es Pläne geben, um das Personal in allen Aspekten der Informationssicherheit zu schulen und um die Schlüsselkonzepte der geringstmöglichen Privilegien, der Kenntnisnotwendigkeit und der Klassifizierung von Informationen je nach Vertraulichkeitsstufe durchzusetzen. Jeder einzelne Mitarbeiter Ihres Unternehmens muss – unabhängig von der Hierarchiestufe – wissen, welche Aufgaben und Verantwortlichkeiten bei der Handhabung vertraulicher Informationen zu beachten sind und welche Maßnahmen in dem Falle zu ergreifen sind, dass ein Mitarbeiter an Informationen gelangt, für die es keine Kenntnisnotwendigkeit gibt. Die beste Schutzmaßnahme gegen Datenlecks besteht in regelmäßigen, umfassenden Schulungen, um sicherzustellen, dass Ihre Mitarbeiter genau wissen, wie vertrauliche Informationen angemessen zu behandeln sind und wie das Unternehmen vor Datenlecks geschützt werden kann. Selbst eine so einfach klingende Vorschrift wie „Bringen Sie keine privaten Datenträger mit auf Arbeit“ kann helfen, versehentliche (oder bewusste) Datendiebstähle oder Datenlecks zu verhindern.

Nutzung optimaler Produkte und Systeme

Glücklicherweise muss sich Ihr Unternehmen bzw. Ihre Behörde den Risiken durch Datenlecks nicht alleine stellen. Partner wie intimus Consulting stehen bereit, um Ihr Unternehmen bei der Entwicklung angemessener Informationssicherungssysteme zu unterstützen und die geeigneten Produkte zur Wahrung der Sicherheit Ihrer Daten zu bestimmen. intimus Consulting assistiert seinen Kunden regelmäßig bei der Umsetzung eines ganzheitlichen Ansatzes zur Informationssicherung. Dazu gehören unter anderem die folgenden Prozesse:

- **Definition von „Sicherheitszonen“ für Informationen**, angefangen von der „öffentlichen“ Zone (Poststelle, Druckerei, Archiv), über die „eingeschränkte“ (interner und externer Schriftverkehr) und die „vertrauliche“ Zone (Vertrieb, Marketing, Einkauf) bis hin zur „hochvertraulichen“ Zone (Führungsetage).
- **Sichere und zuverlässige Vernichtung von Informationen**, um zu verhindern, dass nicht autorisierte Daten nach außen gelangen. Hierzu werden Produkte wie Aktenvernichter, Disintegratoren, Degausser und weitere Geräte zur Datenträgerbereinigung eingesetzt.
- **Risikobewertungen** und Analysen potenzieller Schwachstellen helfen, Verfahren zur Informationssicherung einzurichten und deren Wirksamkeit zu überwachen.
- **Erstellung einer individuellen Risikomatrix** für Ihr Unternehmen, einschließlich der individuellen Risiken für die Informationssicherheit und der potenziellen Kosten im Falle eines Datenlecks.

Schlussfolgerung

Angesichts der zahlreichen Schlagzeilen über „Hacker“ und „Identitätsdiebstähle“ mag der Eindruck entstehen, es handele sich bei dem Thema Informationssicherheit um ein Hightech-Spiel mit dubiosen Akteuren und hochkomplexen Technologien. In Wahrheit jedoch werden die meisten Datenlecks und Verstöße gegen die Informationssicherheit durch ganz normale Mitarbeiter innerhalb des Unternehmens verursacht, die jeweils ihre ganz eigenen Gründe haben, das in sie gesetzte Vertrauen des Unternehmens zu missbrauchen.

Damit Ihr Unternehmen nicht zum nächsten Angriffsziel von WikiLeaks oder ähnlichen Gruppierungen wird, sollten Sie gewisse zentrale Prinzipien beachten. Denken Sie immer daran, dass Ihre Unternehmensgeheimnisse nur so sicher sind, wie dies die am wenigsten vertrauenswürdige Person mit Kenntnis der Informationen zulässt. Erstellen Sie für den Zugriff auf Informationen Vorschriften, Verfahrensweisen und Kontrollmechanismen, statt sich nur den „Technologien zur Informationssicherung“ zu widmen. Und beachten Sie, dass die Informationssicherheit am besten mit einem ganzheitlichen Ansatz gewährleistet werden kann, der alle Aspekte, Risiken und Schwachstellen Ihres Unternehmens einbezieht.

Die Informationssicherheit beruht im Großen und Ganzen auf Vertrauen. Und in jedem Unternehmen gibt es Mitarbeiter, die bereit wären, dieses Vertrauen zu missbrauchen – dies ist allzu menschlich und lässt sich nun mal nicht vermeiden. Ein jedes Unternehmen kann und muss jedoch Vorkehrungen treffen, um einem potenziellen Vertrauensmissbrauch entgegenzuwirken. Nur so lassen sich schwerwiegende Konsequenzen und ein weltweites Bekanntwerden höchst vertraulicher Informationen verhindern.

Unternehmensprofil

Als in den 1960er Jahren die ersten Aktenvernichter eingeführt wurden, war der Begriff Datenschutz noch gänzlich unbekannt. Angefangen mit dem „elektronischen Papierkorb“ INTIMUS Simplex aus dem Jahre 1965 hat sich die Produktpalette stetig weiterentwickelt und erfüllt heute sämtliche Vorgaben und Anforderungen im Bereich der Informationssicherung. Zum Angebot gehören nicht nur Aktenvernichter für klassische Informationsmaterialien wie Ausdrucke, Computerlisten oder sogar vollständige Ordner, sondern auch Maschinen zur Vernichtung von Daten auf modernen Endpoint-Geräten wie CDs, Disketten, Festplatten und Halbleitermedien.

intimus Security Consulting ist ein Konzept zur Unterstützung von Unternehmen weltweit bei der Definition, Umsetzung und Überwachung von Prozessen zur Gewährleistung der Informationssicherheit jenseits von Endpunkten.

Die MARTIN YALE GROUP wurde 2003 aus den zuvor eigenständigen Unternehmen MARTIN YALE Industries (Nordamerika) und Schleicher International (Deutschland) gebildet. Die Gruppe verfügt heute über ein umfangreiches weltweites Vertriebsnetz mit 7 Außenstellen und über 150 Vertriebspartnern.

Kontaktdaten

MARTIN YALE GROUP
Bergheimer Straße 6-12
88677 Markdorf / Deutschland
Tel. 0049 / (0) 75 44 / 60-232
Fax 0049 / (0) 75 44 / 60-248
E-Mail: sattel@martinyale.de
www.martinyale.de