Technical Report

Nr. TUD-CS-2013- 0068

3. April 2013

CASED

IT-Sicherheitstrends kleiner und mittelständischer Unternehmen

Auswertung der Einreichungen des “1. Deutschen IT-Sicherheitspreises für kleine und mittelständische Unternehmen” hinsichtlich IT-Sicherheitstrends

Autoren

Sarah Ahmed, Maximilian Kaiser, Michael Kreutzer

Inhalt

1. IT-Sicherheitspreis für KMU

Der mit insgesamt 5.000 Euro dotierte Preis wurde vom Center for Advanced Security Research Darmstadt (CASED) mit Unterstützung der im Bundesministerium für Wirtschaft und Technologie eingerichteten Task Force „IT-Sicherheit in der Wirtschaft“ erstmalig ausgeschrieben und vergeben.

Ausgezeichnet wurden kleine und mittlere Unternehmen für vorbildliche und praxisnahe Lösungen im Bereich der organisatorischen IT-Sicherheit. Eine Jury aus Vertretern von Wirtschaft und Verwaltung wählte die vier besten anwendungsnahen Konzepte und Lösungen aus den Bereichen Notfallmanagement, Datensicherung, Awareness und Mitarbeitersensibilisierung sowie sichere Netzadministration.

Preisträger sind die artegic AG für ihren besonderen „sicherheitsbezogenen Umgang mit Computern und Software“, die Eventagentur Crossing Mind für ihr beispielhaftes „Datensicherungskonzept“, das IT-Dienstleistungsunternehmen msg services ag für ihre vorbildlichen Aktivitäten im Bereich „IT-Security Awareness” sowie Yildiz CNC-Drehtechnik für ihre Maßnahmen zur „Notfallvorbereitung“.

„Die Lösungen der Preisträger zeigen: IT-Sicherheit in kleinen und mittleren Unternehmen muss nicht kompliziert und teuer sein. Selbst mit überschaubarem Aufwand lassen sich große Sicherheitseffekte erzielen“, sagt Prof. Dr. Michael Waidner, Direktor von CASED.

„Sichere elektronische Geschäftsprozesse in kleinen und mittleren Unternehmen werden immer wichtiger für deren Wettbewerbsfähigkeit. Wir freuen uns daher über die zahlreichen interessanten Einreichungen und die vorbildlichen Sicherheitslösungen der Preisträger und hoffen, dass hierdurch viele Mittelständler zur Nachahmung angeregt werden“, so Hans-Joachim Otto, Parlamentarischer Staatssekretär beim Bundesminister für Wirtschaft und Technologie, anlässlich der Preisverleihung.

1.1. Ausschreibung und Deadline

Der Preis wurde am 03.05.2012 über einen Zeitraum von vier Monaten ausgeschrieben (Fristende war der 31.08.2012).

Potenzielle Teilnehmer wurden über verschiedene Wege auf die Preisausschreibung aufmerksam gemacht. Zum einen informierte ein Consultant einige Firmen direkt, zum anderen sorgte der zusammengestellte Beirat für Verbreitung der Preisausschreibung, weiter verbreitete die Task Force „IT-Sicherheit in der Wirtschaft“ in ihren Netzwerken und die Ausschreibung wurde in einschlägige Foren und an einschlägige Websites gepostet.

Für Unternehmen mit einem Kerngeschäft außerhalb der Informationstechnologie ist das Wissen über die Wichtigkeit von IT-Sicherheit keine Selbstverständlichkeit und deshalb war es für die Preisausschreibung umso wichtiger, gerade diese Betriebe zu einer Teilnahme zu motivieren und die Sensibilität für IT-Sicherheit zu steigern.

1.2. Task Force „IT-Sicherheit in der Wirtschaft“

Die Task Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Technologie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern.

Weitere Informationen unter: **www.it-sicherheit-in-der-wirtschaft.de**

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

2. Übersicht der Einreichungen

Der Jury des IT-Sicherheitspreises für KMU wurden über 20 Bewerbungen zur Bewertung eingereicht, von welchen 19 die Kriterien für eine Zulassung zum Wettbewerb erfüllten. Die einreichenden Unternehmen kommen aus verschiedenen Branchen und sind von unterschiedlicher Größe. Eine Kategorisierung der potenziellen Preisträger mit Unterscheidung einerseits zwischen Anwendern und Dienstleistern und zum anderen zwischen technischen und organisatorischen (Awareness) Lösungen erschien plausibel und praktikabel.

Die Unterteilung der Einrichtungen in die jeweiligen Branchen und Lösungsansätze ist in Tabelle 1 dargestellt.

	Dienstleister	Anwender
Organisation & Awareness	A.3, A.7, A.19, A.13, A.18	A.2, A.12, A.15
Technisch	A.1, A.5, A.6, A.10, A.14	A.4, A.8, A.11, A.16, A.17, A.19

Tabelle 1: Die Nummerierung richtet sich nach den Unterkapiteln des Anhangs A; Quelle: eigne Darstellung

Die Kategorisierung und Zuordnung der Einreichungen entsprechend Tabelle 1 fand erst nach Ablauf der Einreichungsfrist statt, da der Preis erstmalig ausgeschrieben wurde und somit über die Resonanz im Vorfeld nur spekuliert werden konnte. Unmittelbar nach Fristende fand dann das tatsächliche Clustering statt.

3. Auswertung der Themen und resultierende Trends

Vorab muss berücksichtigt werden, dass diese Auswertung der Einreichungen von KMUs nicht repräsentativ ist, da die Anzahl der Einreichungen zur Erreichung dieses Kriteriums zu niedrig war. Mit allen Vorbehalten bezüglich Wissenschaftlichkeit des Vorgehens werden im Folgenden Thesen bezüglich möglicher Trends aufgestellt.

In etwa der Hälfte der Fälle ließen sich die Unternehmen durch externe Dienstleister bei der Einreichung unterstützen bzw. reichten über einen Dienstleister ein, vergleiche Tabelle 1. Dieser Umstand weist darauf hin, dass Unternehmen dieser Größe bereits bei der Formulierung ihrer Sicherheitsbedarfe und -lösungen unsicher sind. Wenn kleine und mittelständische Unternehmen Informationstechnologie als Hilfsmittel zur Unterstützung ihres Kerngeschäftes verwenden, dann ist ihnen dieser Nutzen im Alltagsgeschäft offensichtlich plausibel – wir vermuten allerdings, dass der Nutzen und die Rentabilität von IT-Sicherheitsmaßnahmen ihnen erst nach einschlägigen Vorfällen bewusst werden.

Die Einhaltung der Datenschutzgesetze, -vorgaben und -richtlinien und die damit verbundenen Zertifizierungen scheinen für die Unternehmen wichtig zu sein. Nach unserem Bewertungsschema wurde dieses Thema am häufigsten direkt („+“) und indirekt („O“) adressiert, vergleiche Tabelle 2. Sollte sich dieser Trend empirisch erhärten, dann könnte die These überprüft werden, dass dieses Datenschutz „angekommen“ ist: Die Regulierung von innerbetrieblichem Datenschutz und die Einsicht in ihre Notwendigkeit hat einen hohen Stellenwert in unserer Wirtschaft und Gesellschaft und für Unternehmen lohnt sich der Nachweis ihrer Einhaltung.

Awareness spielt ebenfalls eine große Rolle im Alltag der Unternehmen, dies legt die Bewertung nach Tabelle 2 nahe. Sollte sich dies empirisch erhärten, dann wäre die Kenntnis der Gründe für diese Prominenz von Awareness hilfreich, aktuell lässt sich hierüber nur spekulieren: Haben die Verantwortlichen erkannt, dass technische Maßnahmen nur dann effektiv sind, wenn die Menschen mit eingebunden werden? Oder gibt es einen erhöhten Druck durch einschlägige Vorfälle, beispielsweise eine Häufung von Malware-Einschleusung via social engineering Methoden wie phishing? Oder gibt es andere Gründe?

Dieses Papier gibt erste Hinweise auf mögliche Forschungsthesen. Nur wenn diese Thesen zukünftig auf dem Prüfstand valider empirischer Forschungsmethodik bestehen können, dann hat diese Publikation einen Beitrag geleistet.

Tabelle 2: Kategorisierung der Einreichung hinsichtlich Themen, Legende: „+“ = im Fokus der Einreichung (pro Einreichung wurde ein „+“ vergeben), „O“ = Nebenthema (Mehrfachvergaben pro Einreichung hier möglich), „–“ = Thema spielte bei dieser Einreichung keine Rolle; Quelle: eigene Darstellung

Einreichung	Datenschutz	Awareness	Backup	Policy Enforcement	Internes Informations-management	Fernzugriff	Zugriffs-Management	IT Notfallplan	Sicherheits-analyse	IT-Sicherheits-zertifizierung	
A.1 Umgang mit PC und Software: Kundendaten müssen besonders gesichert sein	+	–	–	O	–	–	–	–	–	–	
A.2 Datensicherungskonzept: Aus Schaden wird man klug	–	O	+	–	–	–	–	–	–	–	
A.3 Awareness: Mit Dr. Jekyll und Mr. Hyde zu mehr Sicherheit im Unternehmen	–	+	–	O	–	–	–	–	–	–	
A.4 Notfallvorbereitung: Auf den Fall des Falles vorbereitet sein	–	–	O	–	–	–	–	+	–	–	
A.5 CamWiki als Wissensdatenbank	–	–	–	–	+	–	–	–	–	–	
A.6 COMPUTENT Secure – Sicherer RDP ohne VPN	–	–	–	–	–	+	–	–	–	–	
A.7 Die Technik allein hilft nicht – Auf die Mitarbeiter kommt es an	–	+	–	–	–	–	–	–	–	–	
A.8 Durchgängiges sicheres Datenzugriffskonzept	O	–	–	+	–	–	O	–	–	–	
A.9 Einführung einer Compliance-Richtlinie für die Einhaltung gesetzlicher Bestimmungen	–	–	–	+	–	–	–	–	–	–	
A.10 Einführung einer Sicheren IT-Infrastruktur bei XCOM AG	O	–	–	+	–	–	O	–	–	–	
A.11 Erstellung und Umsetzung eines Datensicherungskonzeptes	O	–	+	–	–	–	–	O	–	–	
A.12 Ganzheitliches „gelebtes“ Schutzkonzept	+	O	–	O	O	O	–	–	–	–	
A.13 IT-Sicherheitskonzept der Computer-L.A.N. GmbH	+	O	O	O	–	–	O	–	–	–	
A.14 Personalisiertes Server-Zugriffsmanagement	O	–	–	–	–	–	+	–	–	–	
A.15 Sensibilisierungsmaßnahme	O	+	–	–	–	–	–	–	–	–	
A.16 Sichere Organisation und Betrieb einer Informationsplattform für Kunden	+	O	–	O	–	–	–	–	–	–	
A.17 Sicherheitsanalyse anhand kritischer Geschäftsprozesse	–	–	–	–	–	–	–	–	+	–	
A.18 Sicherheitszertifizierung	–	–	–	–	–	–	–	–	–	+	
A.19 Verteilter Datenzugriff bei der Freiwilligen Feuerwehr Mössingen	O	–	O	–	–	+	–	–	–	–	
+	4	3	2	3	1	2	1	1	1	1	19
O	6	4	3	5	1	1	3	1	0	0	24
–	9	12	14	11	17	16	15	17	18	18	147

A Anhang

Zusammenfassungen der 19 Einreichungen in alphabetischer Reihenfolge der Unternehmen, beginnend mit den 4 Preisträgern.

A.1 Umgang mit PC und Software: Kundendaten müssen besonders gesichert sein

Jörg Sayn, Vorstand der artegic AG

Die artegic AG sind Experten für Online CRM und kundenzentriertes Online Dialogmarketing. Das Bonner Unternehmen berät namhafte Kunden bei dem Aufbau und der Gestaltung ihrer Kundenbeziehungen über Online-Kanäle. Dazu zählt E-Mail-Marketing wie auch das Dialogmarketing via SMS und Social Media. Der Umgang mit personenbezogenen Daten und Kundendaten gehört somit zum täglichen Geschäft. „Das bedeutet für uns, dass wir an die Sicherheit sehr hohe Maßstäbe anlegen müssen“, so Jörg Sayn, Vorstand der artegic AG.

Systematische Bewertung, Freigabe und Kontrolle der Software

Eine unternehmensweite Risikoanalyse hat gezeigt, dass die im Haus eingesetzte Software für die Sicherheit der Daten eine entscheidende Rolle spielt, z.B. weil mit ihr personenbezogene Daten oder sonstige vertrauliche Informationen ausgetauscht werden. „Um ganz sicher zu gehen, haben wir Maßnahmen zur systematischen Bewertung, Freigabe und Kontrolle aller eingesetzten Softwareprodukte eingeführt.“ Dazu zählt eine umfangreiche Software-Risikoanalyse, u.a. hinsichtlich:

- unsicherer, fehlerhafter oder bösartiger Software, insbesondere bei Ad-hoc-Installation durch Mitarbeiter
- unsicherer Speicherung von Zugangsdaten, gerade in externen Applikationen
- unbeabsichtigte unverschlüsselte Übertragung streng vertraulicher Daten
- Fehler bei der Verwaltung von Benutzerkennungen durch Mitarbeiter (Mehrfachverwendung, simple Passwörter, keine regelmäßige Änderung)
- Übernahme oder Löschung von Zugängen zu externen Applikationen bei Ausscheiden eines Mitarbeiters

Als Folge wird nun ausschließlich Software aus einer Freigabeliste genutzt. Dies verhindert, dass Software unbekannter Hersteller ohne Prüfung installiert wird. Für jegliche in Betrieb befindliche Software wurden darüber hinaus bestimmte Sicherheitsmerkmale erfasst, dazu gehören u.a.:

- Art und Sicherheit der Authentifizierung (inkl. Optionen zentraler Passwortverwaltung)
- Art der Passwortablage
- Zugriffsberechtigte Personen/Rollen
- Sicherheitsrelevanz der Anwendung (gering bis hoch; in Abhängigkeit der verarbeiteten Daten)

Soweit möglich, wurden die Anwendungen an einen zentralen Login-Dienst angeschlossen. Die Möglichkeit der zentralen Verwaltung wurde zu einem wesentlichen Kriterium neu angeschaffter Software erhoben.

Höchstmöglicher Schutz der Kundendaten

„Unsere systematische Analyse hat in Einzelfällen erhebliche Schwachstellen von Softwareprodukten offenbart. Wir haben vorbeugend geeignete Maßnahmen getroffen und können so einen höchstmöglichen Schutz unserer Kundendaten gewährleisten“, so Jörg Sayn.

Kontakt:

artegic AG
Jörg Sayn
Zanderstraße 7
53177 Bonn
www.artegic.de

Branche: Dienstleister

A.2 Datensicherungskonzept: Aus Schaden wird man klug

Ralf Schönberger, Geschäftsführer von Crossing Mind

Ralf Schönberger ist Geschäftsführer der Lenggrieser Eventagentur Crossing Mind in Oberbayern. Sein Metier ist die Konzeption und Durchführung kreativer Events, Incentives und Trainings.
Besondere Berührungspunkte mit dem Thema IT-Sicherheit hatte Schönberger im Jahr 2007. „Ein Server-Ausfall in Verbindung mit einer unzureichenden Datensicherung führte damals zu einem empfindlichen Datencrash. Als Folge verloren wir einen Auftrag mit 18 Veranstaltungen und einem Umsatzvolumen von ca. 200.000 Euro. Die Kosten für die Wiederherstellung und Neuprogrammierung aller Konzepte, Ideen, etc. beliefen sich unserer Schätzungen nach zusätzlich auf ca. 60.000 Euro. Die Situation war zum damaligen Zeitpunkt existenzbedrohend“, so Schönberger.

Umfangreiches und individuelles externes Datensicherungskonzept

Heute kann dem Unternehmer so etwas nicht mehr passieren. Eine Analyse führte zu dem Schluss, dass in Folge des erforderlichen Zeitaufwandes und der Konzentration auf die Kernkompetenzen eine sichere unternehmensinterne Lösung ungeeignet ist. Daher wurde in Zusammenarbeit mit einem IT-Partner ein umfangreiches externes Datensicherungskonzept entwickelt. Es umfasst:

- Klare und definierte Strukturen innerhalb der Unternehmensorganisation und des ITSystems.
- Regelmäßige (in Abständen von sechs Wochen) Ansprache und Schulung der internen und externen Mitarbeiter.
- Klare, vertraglich geregelte Verantwortlichkeiten des IT-Partners, z.B. Service-Level, Archivierung, Versicherung, etc.
- Verschlüsselte Sicherung aller Daten des Servers auf einem lokalen Backup-Server und zusätzlich Auslagerung (verschlüsselt) in ein Backup-Rechenzentrum bei dem IT- Partner.
  Die Datensicherung erfolgt vollautomatisch und werktäglich.
- Regelmäßige Überwachung der Datensicherung, technisch durch den IT-Partner, Protokollprüfung durch Crossing Mind.
- Teilnahme an sogenannten „Feuerwehr-Übungen“ mit dem IT-Partner, die eine Notfallsimulation inkl. Rückspeicherung der Daten und Wiederanlauf beinhaltet.

Konzentration aufs Kerngeschäft

Das Datensicherungskonzept hat bereits seine Feuertaufe bestanden. Nach einem Serverausfall konnten bereits nach wenigen Stunden alle Systeme und Daten wieder bereitgestellt werden. „Das Sicherheitskonzept, das wir mit unserem Partner entwickelt haben, ist kostengünstig, einfach und sicher und erlaubt uns die Konzentration auf unser Kerngeschäft sowie die ständige Weiterentwicklung unseres Unternehmens“, so Ralf Schönberger.

Kontakt:

Crossing Mind
Ralf Schönberger
Gilgenhöfe 9
83661 Lenggries
www.crossing-mind.de

Branche: Dienstleistung/Eventagentur

A.3 Awareness: Mit Dr. Jekyll und Mr. Hyde zu mehr Sicherheit im Unternehmen

Thomas Soens, Abteilungsleiter und Sicherheitsbeauftragter bei der msg services ag

Die msg services ag mit Sitz in Ismaning/München ist ein IT-Unternehmen und bietet ihren Kunden infrastrukturnahe Dienstleistungen von der Beratung bis zum Betrieb. „Als IT Dienstleister haben wir natürlich auch bei der IT-Sicherheit eine Vorbildfunktion für unsere Kunden. Studien zeigen immer wieder, dass Sicherheitsprobleme häufig durch menschliches Fehlverhalten entstehen. Für uns bedeutet das, möglichst alle Mitarbeiter in die Lage zu versetzen, sich richtig zu verhalten“, so Thomas Soens, Abteilungsleiter und Sicherheitsbeauftragter bei der msg services ag.

Im Unternehmen werden ein umfangreiches Schulungsprogramm sowie Awareness-Kampagnen für alle Mitarbeiter zum Thema IT-Sicherheit durchgeführt. Das Management geht dabei mit gutem Beispiel voran.

Einfach, verständlich und spannend

Erfolgsrezept ist die spielerische Vermittlung des Themas IT-Sicherheit, denn Lernen soll Freude machen. Einfach zu verstehen und eine eingängige und spannende Vermittlung des manchmal etwas trockenen Themas IT-Sicherheit haben in den Schulungen oberste Priorität.

„Beispielsweise wurden zwei Figuren als Maskottchen ausgewählt, die auf allen eingesetzten Informationsmaterialien die Hauptrolle spielen. Es werden Situationen abgebildet, die Sicherheitsmaßnahmen darstellen. Dr. Jekyll, der gute Ratgeber, erzählt, was zu beachten ist, und Mr. Hyde – der ‚Böse' – versucht jede Schwachstelle auszunutzen.“ Zu den Maßnahmen zählen u.a.:

- Regelmäßige Tipps & Tricks für Mitarbeiter rund um IT-Sicherheit.
- Monatliche Nachrichten auf einer Web-Plattform (Intranet), bei Bedarf auch häufiger.
- Monatlicher Versand eines Newsletters (inkl. einer kleinen Story oder eines Vorfalls in den Medien).
- Halbjährige Awareness-Kampagnen mit Postern, Flyern, Quiz.
- Jährliche umfassendere Awareness-Schulung in kleinen Gruppen.
- Das gesamte Themenspektrum vom Virus bis zur Policy.
- Schulungen für Mitarbeiter, die neu ins Unternehmen eintreten.
- Wiederholungsschulungen.

Mitarbeiter kompetent in IT-Sicherheitsfragen

Die Lernfortschritte werden regelmäßig in Tests ermittelt und die Schulungen dem Lernfortschritt angepasst. Die Resultate der Awareness-Kampagne und -Schulungen sind bereits sichtbar. „Einerseits haben wir weniger Sicherheitsprobleme im eigenen Unternehmen, andererseits steigt die Reputation beim Kunden durch aufgeklärte und geschulte Mitarbeiter, die auf Sicherheitsfragen der Kunden kompetent Antwort geben können“, so Thomas Soens.

Kontakt:

msg services ag
Thomas Soens
Robert-Bürkle Straße 1
85737 Ismaning
www.msg-services.de

Branche: Dienstleistung/IT-Dienstleister

A.4 Nofallvorbereitung: Auf den Fall des Falles vorbereitet sein

Recep Yildiz, Geschäftsführer von Yildiz CNC-Drehtechnik

Wenn es um hohe Präzision geht, ist Yildiz CNC-Drehtechnik in Wetzlar eine erste Adresse. Mit 20 Mitarbeitern und drei Auszubildenden stellt das Unternehmen nach Kundenvorgaben Präzisionsdreh- und Frästeile z.B. für die optische und feinmechanische Industrie her. „Als Auftragsfertiger müssen wir auf Kundenanfragen umgehend reagieren, detaillierte Angebote in kürzester Zeit kalkulieren und termingenau liefern. Unser Geschäft wird immer schneller“, so Recep Yildiz, Geschäftsführer von Yildiz CNC Drehtechnik.

Notfallvorsorge ist Überlebensfrage

Ein Ausfall der IT – sei es für die Angebotserstellung, die Kommunikation mit Kunden, die Qualitätssicherung im Messlabor oder zur Steuerung der Dreh- und Fräsmaschinen – kann existentielle Folgen haben. „Für mein Unternehmen ist das reibungslose Funktionieren der IT eine Überlebensfrage“, so der Geschäftsführer.

Um auf alle Fälle vorbereitet zu sein, hat der Unternehmer vorgesorgt und mit Hilfe eines IT-Dienstleisters ein ausgeklügeltes System zur Notfallvorsorge etabliert:

- Alle zur Re-Installation der Softwaresysteme notwendigen Angaben (IDs, Authentifizierungsdaten, Lizenzinformationen und Installationsanweisungen) werden in Papierform sicher verschlossen und übersichtlich vorgehalten.
- Ein Notfall-PC wurde eingerichtet (Laptop) mit E-Mail-System, Kalkulationssoftware inkl. Software für Angebots- und Lieferscheinerstellung.
- Bei Ausfall der Internetverbindung (E-Mail) kann über Mobilfunk (USB-Stick) gearbeitet werden.
- Bei Ausfall des Werkstattrechners oder des Messplatzes können die Systeme und Daten kurzfristig auf Ersatz-Hardware (Standard-PC) installiert werden.
- Ein Vorgehensplan (Abfolge) im Notfall liegt schriftlich vor und wird regelmäßig aktualisiert.

Produktions- und Lieferausfällen vorbeugen

„Durch die Notfallvorsorge sind wir in der Lage, innerhalb von einer Stunde für unsere Kunden wieder ansprechbar zu sein. Das Risiko des Verlustes von Aufträgen aufgrund der Nichtverfügbarkeit von IT ist minimiert“, so Recep Yildiz.

Kontakt:

Yildiz CNC-Drehtechnik
Recep Yildiz
Am Schmittenberg 14
35578 Wetzlar
www.yildiz-drehtechnik.de

Branche: Produzierendes Gewerbe/Dreh- und Frästechnik

A.5 CamWiki als Wissensdatenbank

Harry Kurschat

CamData GmbH

Konzept

Wir haben das Produkt "MediaWiki" zunächst als Wissensdatenbank und nach einiger Zeit als Qualitätsmanagement-Handbuch (abgenommen vom Auditor gemäß ISO 9001:2008) eingesetzt. Als IT-Dienstleister verfügen alle unsere Mitarbeiter über einen EDV-Arbeitsplatz. Jeder Mitarbeiter hat einen eigenen Zugang zum "CamWiki" (Zugang nur mit Username und Passwort).
Sinn und Zweck dieser Maßnahme ist es Firmenwissen zentral unter einem Produkt zu verwalten. Anweisungen, Richtlinien, Informationen, Ansprechpartner, Beschreibungen von Arbeitsabläufen (intern wie extern), Notfallpläne, ToDo´s bei bestimmten Vorfällen usw. werden zentral im CamWiki gesammelt und nach eingehender Recherche aussortiert, ausgebessert und in entsprechenden Kategorien zur allgemeinen Nutzung abgespeichert.

In einer Betriebsversammlung wurde das CamWiki dann als Firmenhandbuch/Arbeitsrichtlinie verabschiedet. Jeder neue Mitarbeiter wird auf dieses CamWiki verpflichtet. Neue Dokumente können durch jeden Mitarbeiter (mit Zugang) erstellt werden. Wöchentlich werden die neuen Dokumente durch die Abteilungsleiter überprüft und freigegeben.

Nutzen

Keine doppelte Datenhaltung mehr, neueste Informationen jederzeit verfügbar (Techniker sowie Vertrieb haben per Tunnel Zugriff auf das Intranet/CamWiki). Bestimmte Arbeiten werden als Handbücher/Vorlagen hinterlegt und können für kundenspezifische Arbeiten benutzt und umgeschrieben werden (das Rad muss nicht neu erfunden werden). Änderungen können sofort im Dokument getätigt werden und sind danach in Echtzeit für alle Mitarbeiter einzusehen. Jede Änderung an einem Dokument wird dokumentiert (Name, Datum, Uhrzeit, Art der Änderung, ...) und ist für den CamWiki-Admin ersichtlich.
Neue Mitarbeiter haben ein Handbuch für Ihre Tätigkeiten zur Verfügung, weil hier auch tägl. Arbeiten niedergeschrieben werden.

Zugriff auf Daten im Intranet sowie Internet sind jederzeit möglich

Durch Verlinkungen im Dokument sind diese Links direkt erreichbar. Der User muss nicht in den Medien hin- und herspringen. Selbst die Handhabung des CamWiki ist im CamWiki hinterlegt (Erstellung, Prüfung, Freigabe, Änderung, Verteilung, Rücknahme und Archivierung von Dokumenten).

Kontakt:

CamData GmbH
Harry Kurschat
Eickener Strasse 133
41063 Mönchengladbach
www.camdata.de

Branche: EDV-Dienstleister

A.6 COMPUTENT Secure - Sicherer RDP ohne VPN

Corinna Göring

COMPUTENT GmbH

Konzept

Mobilität am Arbeitsplatz ist nicht nur ein Schlagwort, sondern gewinnt für die Chefetagen oder Außendienstmitarbeiter immer mehr an Bedeutung. Gerade für den KMU Bereich wird es immer mehr existenziell. Dabei bekommen auch die EDV-Betreuer zunehmend die Aufgabe, bei Problemen umgehen auf das EDV-System Einfluss nehmen zu können. Und am Besten sollen beide Aufgaben in einer Komponente zusammengefasst werden, um den Hardwareeinsatz zu reduzieren. Dabei muss zusätzlich sichergestellt sein, dass keine relevanten Firmendaten in falsche Hände geraten. Es werden dazu bereits mehrere Lösungen am Markt angeboten:

- Fernwartungssoftware: erfordert größtenteils eine Installation auf dem Gast-Rechner und es ist ein Server zwischengespeichert, dessen Zugriffssicherheit und Datensicherheit man selbst nicht beeinflussen kann. Bei deren Nutzung müssen Sie dem Anbieter und dessen Sicherheitskonzept vertrauen, da die Daten auf Servern außerhalb Ihrer Einflusssphäre liegen
- VPN baut einen sicheren Tunnel auf, der allerdings einen speziellen (meist teuren) VPN-Router erfordert, sowie auf den Gast-PCs installierte VPN-Clients. Man ist dadurch gerätegebunden. Die EDV-Betreuer haben die Herausforderung, dass mehrere unterschiedlicher VPNs Clients diverser Kunden nicht auf einem Gerät ohne Probleme zu installieren waren. Der Kunde ist auch immer an die Hardware gebunden. Firmen müssen Ihren externen Mitarbeitern vorbereitete Geräte zur Verfügung stellen.
- RDP Zugriff über Web: eine sehr unsichere und doch oft genutzte Form, da die Eingaben der URL, des Benutzers und Passworts durch Keylogger ausspioniert werden können. Mit diesen ausgespähten Zugangsdaten ist dann ein ungehinderter Zugang möglich.
- RSA-Token: für den Zugriff wird ein Einmalpasswort vergeben. Dazu muss eine Infrastruktur in der Firma aufgebaut werden und es fallen monatliche Kosten an. Zur Installation ist ein gewisses Know-How erforderlich, was sich in den Installationskosten niederschlägt.

Fazit: Unsere Idee war einen eigenen flexiblen sicheren Fernzugriff für KMUs zu entwickeln, der unabhängig vom Endgerät genutzt werden kann. Dieser soll gleichermaßen dem Kunden, wie auch den IT-Systembetreuern Vorteile bringen. Das Ganze haben wir in Eigenregie ohne Fördermittel auf den Weg gebracht.

Mit der Secure Box und dem USB-Stick als Key können Kunden unterwegs ohne Client Installation von jedem beliebigen Windows PC mit Ihren Datenbanken, Ihrem Kalkulationsprogramm und anderen Anwendungen produktiv arbeiten, als wenn Sie im Büro vor dem PC sitzen. Eine Box hinter dem Router handelt die Benutzerrechte. Die Installation erfolgt in ca. 30 Minuten. Der Kunde oder Techniker hat unterwegs nur einen speziellen USB-Stick in der Tasche, den er einfach an die USB Schnittstelle im Hotel, Internet Café, Daheim oder beim Kunden anstecken kann. Die Lösung baut dann einen 2048-Bit verschlüsselten SSH Tunnel ins Firmennetz auf. Durch eine Hardwarekodierung und das mehrstufige Sicherheitssystem stellt die Lösung sicher, dass Daten auch dann nicht in falsche Hände geraten, wenn der Stick verloren geht. Wichtig ist uns dabei auch die Kostenreduzierung. Die Hardware im Firmennetz muss nicht ausgetauscht werden. Es wird lediglich ein freier Port in dem bestehenden Router benötigt.

Seit 2 Monaten kann man die Box auch in Verbindung mit dem iPad nutzen. Den kompletten Windows Desktop über Maussteuerung mit dem iPad bedienen. In der Entwicklung befinden sich noch Android und Mac Clients sowie WakeOnLan.

Nutzen

Durch die COMPUTENT Secure Lösung ergibt sich ein hoher Nutzen für Unternehmen und Systembetreuer! Ein Produkt für zwei Aufgabenstellungen.

Trotz der einfachen flexiblen Handhabung ist ein Maximum an Sicherheit gegeben. Der Kunde muss an seiner Struktur in der Firma nichts ändern. Es ist kein Austausch des Routers erforderlich. Unsere Lösung kann auch zusätzlich zu VPN implementiert werden. Der Kunde kann den externen Zugriff Variabel durch Vergabe des USBSticks an mehrere Mitarbeiter lösen. Die Firmen müssen keine Geräte für Ihre externen Mitarbeiter mehr vorinstallieren und vorhalten, sondern die Mitarbeiter könnten theoretisch eigene Systeme (BYOD) verwenden. Dadurch gibt es praktisch keine Ausfallzeiten mehr, da bei Defekt eines Gerätes sofort ein anderes verwendet werden kann.

Man kann von jedem beliebigen Windows-PC, der eine USB-Schnittstelle besitzt und über Internetzgang verfügt, ins Firmennetz oder auf den Firmen-PC. Eine Installation von Software auf dem Gast-PC ist nicht notwendig. Dadurch ist einfachstes Handling für den User gegeben. Einfach den USB-Stick anstecken, Passwort eingeben und der SSH-Tunnel baut sich auf. Der Zugang ist von Daheim, externen Büro, Hotel-PC oder vom Kundenrechner möglich, ohne darauf Spuren zu hinterlassen. Der Fernzugriff erspart zudem doppelte Datenhaltung und doppelte Datenpflege. Der spezielle USB-Stick ist hardwarekodiert und nicht kopierbar. Bei Einrichtung wird jeder Stick einem Benutzer zugeordnet. Der 2048 Bit (RSA) SSH-Tunnel ist mind. 30-50 % schneller als VPN, da der Protokoll-Overhead des SSH-Tunnel deutlich geringer ist. Es ist kein Server zwischengeschaltet. Direkter Aufbau eines Tunnels zwischen Firma und Mitarbeiter.
Aufwendige Definierung von Firewallregeln ist nicht notwendig, da jedem Benutzer eine eindeutige Anwendung zugeordnet wird.

Durch die 2-Faktor-Authentifizierung können auch Keylogger den User nichts anhaben, da der Hacker zusätzlich den USBStick benötigt. Der Fernzugriff ist nur in Verbindung mit dem Stick möglich.
Die Systembetreuer können mit einem USB-Stick (Lizenz) alle Kunden betreuen, die diese Box in ihrem Firmennetz installiert haben. Die Kunden müssen die Technikerlizenz nicht extra bezahlen.
Ein großer Nutzen für kleine und mittelständische Unternehmen ist die Kostenstruktur. Ein geringer Anschaffungspreis (Einstiegsvariante 345,- netto) und keine monatlichen Kosten.

Im nächsten Update wird Wake-On-LAN implementiert, so dass ein ausgeschalteter Rechner über die Lösung eingeschaltet werden kann. Dieses bietet bisher kein Mitbewerber.

Die Einrichtung der Box erfolgt einfach und komfortabel über ein browserbasiertes Konfigurationsmenü. Zeitaufwand ca. 30 Minuten. Administratoren können flexibel einstellen, auf welche IP-Adressen, Ports und Ressourcen zugegriffen werden darf. Es können einem Benutzer auch mehrere-USB-Sticks zugeordnet werden und die Sticks können in der Box schnell an- und abgemeldet werden. Über Log-Dateien lässt sich jeder Zugriff auf Benutzer-Basis und anhand des verwendeten Sticks nachvollziehen.

Ohne 2-Faktor Authentifizierung ist nun auch die Nutzung der beliebten iPads im Unternehmen im vollen Umfang sicher möglich durch die Remoter VNC App.

Kontakt:

COMPUTENT GmbH
Corinna Göring
Leipziger Str. 13/15
86833 Ettringen
www.computent.de

Branche: Unternehmens-IT gewerblicher Kunden

A.7 Die Technik allein hilft nicht – Auf die Mitarbeiter kommt es an

Monika Egle, Rolf Strehle

ditis Systeme, NL JMV GmbH & Co. KG

Konzept

Es wurde ein Modell für Awareness Kampagnen im Bereich Informationssicherheit und Datenschutz entwickelt, das es mittelständischen Unternehmen erlaubt, auf Basis eines Kosten effizienten Baukastenprinzips, Awareness Kampagnen durchzuführen und einen fortlaufenden und nachhaltigen Prozess der Awareness im Bereich der Informationssicherheit und des Datenschutzes zu etablieren.

Auf die Umsetzung kommt es an!

Knackpunkt einer jeden Awareness-Kampagne ist natürlich deren Umsetzung. Sie entscheidet über Erfolg und Misserfolg. Deshalb sollten hier die einzelnen Maßnahmen genau geplant und auf Praktikabilität und Nachhaltigkeit überprüft werden. Eine Vorgehensweise im vier Phasen Modell hat sich in der Praxis als sehr erfolgreich erwiesen.

Das Modell in der Praxis

Im Nachfolgenden wird die Umsetzung der einzelnen Phasen beschrieben:

Phase 0 „Vorbereitung“: Vor dem Start gut planen!

In dieser Phase werden elementare Grundlagen geschaffen, die auf alle weiteren Phasen ihre Auswirkungen haben. Hierzu gehören die Sensibilisierung des Topmanagements, die Definition der Verantwortlichkeiten, der Leitgedanke und ein Signet sowie ein konkreter Aktionsplan.

Die ditis hat hier insbesondere einen mehrsprachigen Baukasten aus Flyer, Poster, Online-Plattform, E-Learning, Filme und Giveaways entwickelt, der als Grundlage individuell und doch kosteneffizient in die Planung einer Awareness-Kampagne einfließen.

Phase 1 „Auftakt“: Der Paukenschlag - die Kampagne beginnt

Um eine möglichst hohe Aufmerksamkeit im Unternehmen für die Awareness-Kampagne zu wecken, wird eine zweigleisige

Herangehensweise für die Auftaktphase empfohlen:

1. Allgemeine Bekanntmachung: Das Thema Informationssicherheit und Datenschutz sowie die Ansprechpartner werden über die Medien bekannt gemacht: Mitarbeiterzeitung, Plakate am Schwarzen Brett, Hinweis auf der Startseite des Intranet, bestehende Newsletter-Plattformen.
2. Events vor Ort - der Security Day: Lokale Events, die sogenannten Security Days, werden durchgeführt. Durch diese Präsenzveranstaltung vor Ort bekommt das Thema Informationssicherheit und Datenschutz ein Gesicht. Das Kampagnen-Team kommt mit den Mitarbeitern ins Gespräch und erhält direktes Feedback zu Problemen im Alltag. Die Security Days werden ähnlich einer Roadshow sequentiell geplant. Die mehrsprachigen Bausteine des Awareness Baukasten unterstützen das Kampagnen-Team auch bei der Durchführung an internationalen Standorten.

Phase 2 „Wissen vermitteln“: Übergang in einen kontinuierlichen Prozess

Um Wissen erfolgreich zu vermitteln, werden zielgruppenorientierte Aktionen zu speziellen Fachthemen, wie beispielsweise Verschlüsselung, Mobility, sicherer Zugang zum Unternehmensnetz, sicherer Datenaustausch gestartet. Auf das jeweilige Fachthema ausgerichtete Werkzeuge aus dem Awareness-Baukasten kommen hier zum Einsatz.

Phase 3 „Wissen verstärken“: Unterstützung bereits bestehender Prozesse

In der Phase 3 werden Maßnahmen aus dem Awareness-Toolkit in bestehende Prozesse eingebunden wie beispielsweise:

- Einstellung neuer Mitarbeiter
- Auslieferung mobiler Geräte (Handy, Laptop, UMTS-Karte)
- Bereitstellung von Zugängen zum Unternehmensnetz (WLAN, Modemanschlüsse, VPN)
- Reisebuchungen

Nutzen

Für den Erfolg einer Awareness-Kampagne sind viele Faktoren entscheidend. Eines muss jedoch besonders herausgehoben werden:
„Awareness schaffen“ muss als fortlaufender Prozess angelegt sein, um nachhaltig zu wirken. Daher ist es wichtig, den Mitarbeitern über permanente Informationssysteme konkrete Unterstützung in ihrem Arbeitsalltag zu bieten. Bestehende und etablierte Medien wie beispielsweise Mitarbeiterzeitung, Newsletter und Intranet müssen in Aktionen eingebunden werden. Diese Awareness-Aktionen müssen in den Kontext bestehender Prozesse integriert werden. Wenn ein Unternehmen diese Regeln befolgt, lässt sich über eine Awareness-Kampagne das Niveau von Informationssicherheit und Datenschutz enorm steigern.

Die ditis hat hierfür ein Konzept und einen mehrsprachigen Baukasten aus Flyer, Poster, Online-Plattform, E-Learning, Filme und Giveaways entwickelt, das es auch kleineren und mittelständischen Unternehmen ermöglich, nachhaltig Awareness als fortlaufenden Prozess im Unternehmen zu etablieren. Durch die Synergie-Effekte über unterschiedliche Unternehmen hinweg wird ein kosteneffizienter Weg zur Schaffung von Awareness möglich.

Das Konzept und der Baukasten sind schon heute bei unterschiedlichen mittelständischen Unternehmen im Praxis Einsatz und werden fortwährend erweitert.

Kontakt:

ditis Systeme, NL JMV GmbH & Co. KG
Monika Egle, Rolf Strehle
Carl-Schwenk-Straße 4-6
89522 Heidenheim
www.ditis.de

Branche: IT-Sicherheit und Datenschutz

A.8 Durchgängiges sicheres Datenzugriffskonzept

Jens-Oliver Müller

Kleymann, Karpenstein & Partner

Konzept

Als Anwaltskanzlei und Notariat sind wir mit sensitiven Daten unserer Klienten befasst. Diese Daten müssen bei Bedarf auch unmittelbar zur Verfügung stehen Deshalb steht der Schutz der Vertraulichkeit der Daten für uns an erster Stelle.
Bei KKP sind aus IT-Sicht 2 Anwendergruppen tätig: 18 Anwälte und 20 Sachbearbeiter. Alle Benutzer der Kanzlei arbeiten über eine Terminalserversitzung, ohne die Möglichkeit der lokalen Speicherung der Daten. Somit ist gewährleistet, dass keine Daten abgezogen, oder durch Verlust eines Notebooks abhandenkommen können.
Die IT-Infrastruktur unterstützt das Konzept, dass alle Nutzdaten auf mehreren Servern gehalten und auch prozessiert werden (Terminal-Server-Konzept), gleich, ob der Anwender im Büro sitzt oder mobil (über VPN) arbeitet.

Maßnahmen zur Organisation des Datenzugriffs

- Bei Eintritt und Austritt eines Mitarbeiters wird nach einem definierten Prozess verfahren. Beim Eintritt wird der „Benutzer“ angelegt, Zugriffsrechte basierend auf Fachgebiet und Abteilung werden zugewiesen und ein über Gruppenrichtlinien gesteuertes, serverbasierendes Profil erstellt. Dieser Prozess stellt sicher, dass nur auf die Daten zugegriffen werden kann, die für die konkrete Leistungserfüllung benötigt werden. Beim Austritt werden alle Daten des Benutzers archiviert, das Profil, sowie alle Zugangsberechtigungen entfernt.
- Der Status des Datenzugriffskonzeptes wird regelmäßig überprüft und den wachsenden Bedürfnissen der Mitarbeiter angepasst.
- Der Zugang zum gesamten System ist passwortgeschützt, deren Güte und Lebenszyklen durch eine Richtlinie bestimmt wird (Beispiel: Länge des Passwortes mit mind. 8 Zeichen, alphanumerisch und mind. 1 Sonderzeichen, 6 Wochen Gültigkeit und Historie mit 12 Wechselzyklen. Die Einhaltung dieser Richtlinie wird technisch erzwungen.
- Die Richtlinien sind so definiert, dass es Mitarbeitern nicht möglich ist, während einer Terminal-Server-Session Daten auf der lokalen Festplatte oder sonstigen angeschlossenen Wechselmedien zu speichern.
- Innerhalb der Kanzlei sind alle Netzverbindungen kabelgebunden, WLAN ist ausgeschlossen.
- Für die Mitarbeiter an den stationären Arbeitsplätzen ist die Privatnutzung von Internet und Email durch Betriebsvereinbarung untersagt.
- Die komplette Emailkommunikation wird revisionssicher archiviert und kann im Bedarfsfall nach dem 6-Augenprinzip eingesehen werden. Der externe Emailverkehr über webbasierende Clients, wie Google,- Webmail wird durch eine Firewall Regel unterbunden.
- Physische Akten sind vor dem Verlassen des Büros vor unbefugtem Einblick zu sichern.
- Der Publikumsverkehr ist so organisiert, dass Besuchern nur Zutritt zu speziellen Bereichen (Foyer, Besprechungszimmer) gewährt wird, wo sie weder Bildschirme einsehen, Druckerausgaben sichten oder unbefugt Akten einsehen können.
- Darüber hinaus regelt eine Betriebsvereinbarung die Schweigepflicht der Mitarbeiter über das Verlassen der Kanzlei hinaus.

Sensibilisierung und Schulung der Mitarbeiter

- In regelmäßigen Abständen finden Workshops in der Kanzlei zu IT-Sicherheit und Datenschutz durch die Geschäftsleitung, sowie eines externen Datenschutzbeauftragten statt
- Anwendungsspezifische Schulungen werden ebenfalls regelmäßig durchgeführt

Nutzen

Die Verantwortung von KKP als Anwalts,- und Notariatskanzlei erfordert bereits von Gesetzes wegen höchste Sicherheitsstandards beim Umgang mit Daten von Mandanten sowie Mitarbeiterdaten.

Die umgesetzten Maßnahmen

- Unterstützten die Mitarbeiter bei der Einhaltung der anwaltlichen Verschwiegenheitspflicht
- Erleichtert den Umgang mit Hard,- und Software
- Vermeidet „Wildwuchs“ bei Anwendungssoftware
- Erleichtert die Administration (keine Turnschuhadministration)
- Sind auch „Marketinginstrument“
- Unterstreicht die Kompetenz im IT-Recht

Kontakt:

Kleymann, Karpenstein & Partner
Jens-Oliver Müller
Philosophenweg 1
35578 Wetzlar
www.kleymann.com

Branche: Wirtschafts- und Kommunalkanzlei

A.9 Einführung einer Compliance-Richtlinie für die Einhaltung gesetzlicher Bestimmungen

Andreas Liefeith, Uwe Seiler, Steffen Scholz

procilon GROUP

Konzept

Einführung einer Compliance-Richtline für die Einhaltung gesetzlicher Bestimmungen, regulatorischer Standards und der Erfüllung weiterer, wesentlicher vom Unternehmen selbst gesetzter ethischer Standards und Anforderungen.

Die Richtlinie gilt für alle bei der procilon GROUP (nachstehend nur „procilon“ genannt) beschäftigten Mitarbeiter, Geschäftsführer und leitende Angestellte. Sie gilt darüber hinaus für Vertreter, Consultants, Geschäftspartner und sonstige Dritte, mit denen die procilon eine dokumentierte Vertragsbeziehung aufgenommen hat.

Innerhalb der Richtline spielt das Thema IT-Sicherheit eine wichtige Rolle und umfasst die Themen:

- Lizenzen/Netzwerküberwachung/Archivierung
- Datensicherung
- Notfallplan/Verantwortlichkeiten/infizierte Mails
- Datenschutz(hier besonders):
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle
  - Weitergabekontrolle
  - Eingabekontrolle
  - Auftragskontrolle
  - Verfügbarkeitskontrolle
  - Trennungsgebot

Nutzen

Sehr großer Nutzen wegen Referenzierbarkeit auf Kundenprojekte.

Kontakt:

procilon IT-Logistics GmbH Andreas Liefeith Leipziger Straße 110 04425 Taucha www.procilon.com	proinsys IT-Systemhaus GmbH & Co. KG Uwe Seiler Leipziger Straße 110 04425 Taucha www.proinsys.de	procilon IT-Solutions GmbH Steffen Scholz Leipziger Straße 110 04425 Taucha www.procilon.com

Branche: IT-Sicherheits-Lösungen für Unternehmen, Institutionen und öffentliche Einrichtungen

A.10 Einführung einer Sicheren IT-Infrastruktur bei der XCOM AG

Martin Seufert, Roland Heydkamp

XCOM AG

Konzept

Als IT-Dienstleister für die Finanzindustrie arbeitet die XCOM mit hochsensiblen Daten, deren Sicherheit an erster Stelle steht. Ein Verlust solcher Daten käme einer Katastrophe gleich: der Reputationsschaden für die XCOM mit der Hauptzielgruppe Banken wäre nicht mehr reparabel. Wir haben daher für uns festgestellt: Wir wollen und müssen auf unsere Daten aufpassen, denn sie stellen unseren Firmenwert dar.

Daher hat die XCOM vor gut 1 ½ Jahren begonnen, einen Leitfaden für die höchstmögliche Absicherung der IT zu entwickeln und diesen Weg konsequent fortgeführt. Folgende Ziele wurden definiert:

- Alle auf Hardware gespeicherten Informationen sollen verschlüsselt werden
- Jegliche Kommunikation soll verschlüsselt werden
- Es soll eine PKI-Struktur mit x509 Zertifikaten aufgebaut werden
- Die Authentifizierung soll ohne Passwort mit Smartcards erfolgen
- Es sollen keine Schlüssel mehr auf Systemen gespeichert, sondern auf Smartcards aufgebracht werden

Es wurde eine eigene hochsichere Public Key Infrastruktur aufgebaut, die die Basistechnologie für zertifikatsbasierte Sicherheitsleistungen und Produktion von Smartcards bereit stellt. So können Integrität und Vertraulichkeit der Daten sowie eine aussagekräftige Authentizität/Identifikation in der elektronischen Kommunikation erreicht werden. Die PKI besteht aus den folgenden Bestandteilen:

Zertifizierungsstelle:
META und SUB Certificate Authority (CA)
Client Server Zertifikat Authentifizierung (SSL/TLS)
Verschlüsselte Kommunikation per Web (SSL/TLS)
Zertifikatsbasierter VPN Zugang (OpenVPN mit OTP)
Verschlüsselte Kommunikation per E-Mail (S/MIME)

Registrierungsstelle:
Certificate Signing Request

Zertifikatsperrliste:
Certificate Revocation List
Online Certificate Status Protocol

Verzeichnisdienst:
Directory Service

Organisatorisch:
PIN-Mailer
dedizierter Speicher für die Zertifikats Auslieferung
Reporting/Auditing

Die CA enthält die Root Instanz des Systems. Alle beschriebenen Schlüssel und Zertifikate können nur hierauf erstellt und auf Smartcards aufgebracht werden. Des Weiteren werden die PIN Briefe erstellt. Die CA ist in einem abgesicherten Bunker untergebracht und mit unterschiedlichen Schlüsseln versehen, die in der Hand von unterschiedlichen MA aus unterschiedlichen Abteilungen liegen. Keine dieser Abteilungen/MA kann für sich allein das System starten oder Karten produzieren. Die Erstellung o.g. Userzertifikate bedürfen der PIN Eingaben von min. 3 MA.

Das zentrale Rückgrat besteht aus einem Kerberos- und einem LDAP Server. Diese beiden Systeme übernehmen

- Authentifizierung: Feststellen & Beglaubigen der Identität (Kerberos)
- Autorisierung: Zugriff zu einem Dienst erlauben oder verbieten (LDAP)
- Auditing: Aufzeichnen aller Aktivitäten aus den beiden vorher genannten (Kerberos)

Jeder XCOM-MA bekommt eine eigene Smartcard sowie einen PIN-Brief mit einer 6-stelligen PIN und 8-stelligen PUK, deren Unversehrtheit und Empfang er dem Personalbüro gegenüber bestätigen muss. Sobald das Schreiben vorliegt, wird LDAP freigeschaltet (mit LDAX). Jeder MA erhält einen Stufe 3-Leser Reiner SCT cyberJack e-com plus und kann sich mit Karte und PIN an seinem Gerät authentifizieren.

Bei mobilen Devices findet der Zugang mittels Zertifikat-basierter Authentifizierung und einer One Time Password (OTP) Authentifizierung statt. Das Endgerät wird zum Token Generator. Die benötigten Komponenten wie MOTP-Server, OpenVPN, Offline MOTP APPS für die Endgeräte sind Open Source Produkte.

Nutzen

Die Sichere Infrastruktur der XCOM AG schafft für uns selbst und als Angebot auch für kleine und mittelständische Unternehmen eine größtmögliche Sicherheit vor Spionage, Datenverlust und Datendiebstahl.

Die Lösungsbausteine sorgen für:

- Sicherheit durch vollständige Verschlüsselung der Festplatten
- verschlüsselte Kommunikation (intern und extern)
- verschlüsselte Verbindungen zu den Daten
- sichere Anmeldung am hausinternen Netz
- verschlüsselte Datensicherung
- Entkopplung der Schlüssel von Login und Profil
- passwort-unabhängige Freigabe der Schlüssel
- 2-Faktor-Authentifizierung (Haben und Wissen)

Kostenminimierung durch:

- Einsatz von Open Source für alle relevanten Anwendungen
- Nutzung von preisgünstigen Alternativen für Zertifikats-Services

Vereinfachung durch:

- eine einzige Anmeldung für alle Anwendungen und Dienste
- die richtigen Zugriffe für jeden User an allen Geräten
- die Vermeidung weiterer aufwändiger Sicherheitsmaßnahmen bei der Arbeit

Die produzierten Smartcards lassen sich zudem auch für weitere Dienste nutzen (z.B. als Mitarbeiterausweis, für die Zeiterfassung oder als Bezahlsystem für die Kantine).

XCOM setzt, soweit dies möglich ist, Open Source Software ein.

Das hat Vorteile für den Anwender:

- Die Investitionskosten können auf ein Minimum reduziert werden
- Individuelle Anpassungen sind einfacher
- Sicherheitslücken werden durch die Community schneller geschlossen
- Die Software ist transparenter, so dass insbesondere bezüglich der Sicherheit jeder Programmschritt nachvollziehbar ist.

Kontakt:

XCOM AG
Martin Seufert
Bahnstr. 37
47877 Willich
www.xcom.de

XCOMpetence AG
Roland Heydkamp
Bahnstr. 37
47877 Willich
www.xcompetence.de

Branche: IT-Dienstleister für die Finanzindustrie

A.11 Erstellung und Umsetzung eines Datensicherungskonzeptes

Holger Fuchs

...iutax Steuer & Recht

Konzept

Erstellung und Umsetzung eines Datensicherungskonzeptes mit externer Unterstützung

Unser Anforderungsprofil an IT und Datensicherung ist denkbar einfach: Wir wollen mit IT-Problemen nichts zu tun haben. IT muss laufen! Unser „Geschäft“ ist die Steuer- und Rechtsberatung und nicht die IT. Wir brauchen eine sehr sichere Lösung bei niedrigen Kosten. Diese Aufgabe haben wir an unseren langjährigen IT-Partner delegiert und „outgesourct“, da wir nicht über die dafür notwendige Expertise und Ressourcen im Haus verfügen.
Die Firma aobis begleitet uns in allen Fragen zum Thema IT als Full-Service-Dienstleister seit unserer Gründung im Jahre 2006. Wir haben dabei im Laufe der Jahre verschiedene Sicherungskonzepte entsprechend dem technischen Fortschritt umgesetzt.
Unterstützt wird die Lösung durch unser IT-Konzept mit Terminal-Server-Lösung, welches erzwingt, dass Daten nur auf Servern abgelegt werden, die dann vollständig in die Datensicherung eingebunden sind. Die jetzige Lösung hat sich bei einem Hardware-Ausfall bereits bewährt. Die Ausfallzeiten sind minimal. Unseren und den Ansprüchen unserer Mandanten wird damit voll Genüge getan. Unsere IT-Datensicherheit haben wir mit minimalstem Wartungsaufwand und günstigen Kosten sichergestellt.

Intern unterstützen wir unseren externen Partner durch Beteiligung bei Übungen und Sensibilisierung der Mitarbeiter. Das Datensicherungskonzept beinhaltet die Beschreibung der Verantwortlichkeiten, Art, Umfang und Häufigkeit der Sicherung, den Schutz der Übertragungswege und der Sicherungsdateien. Darüber hinaus verlangt das Konzept die Prüfung der Datensicherung und Übung der Rücksicherung.

In der konkreten Umsetzung

- sind die Verantwortlichkeiten des externen Partners und die Service-Level vertraglich vereinbart
- werden alle Daten (der ausgewählten Geräte laut Konzept) gesichert
- werden alle Daten auf einem lokalen Backup-Server verschlüsselt gesichert
- erfolgt die Datensicherung vollautomatisch und werktäglich
- wird die Datensicherung regelmäßig überwacht. Unser Dienstleister überwacht dies technisch, wir prüfen die Protokolle.

- werden regelmäßige Wiederherstellungstests durchgeführt
- werden die Daten zusätzlich in ein Backup-Rechenzentrum bei unserem Partner ausgelagert
- werden die Daten vor der Auslagerung mit AES 256bit verschlüsselt
- erfolgt die Übertragung der Daten ins Rechenzentrum über eine verschlüsselte Leitung
- werden regelmäßig Desaster-Recovery-Simulationen durchgeführt

Nutzen

IT-Datensicherheit ist für die Kanzlei iutax eine existentielle Frage. Gesetzliche Aufbewahrungsvorschriften sehen vor, Unternehmensdaten für zehn Jahre aufzubewahren. Wir müssen folglich gewährleisten, dass unsere Mandanten ihre kompletten Unternehmensdaten der vergangenen zehn Jahre auf Abruf zur Verfügung haben.

Unser Nutzen:

- Reputation als verlässlicher Partner
- Konzentration auf das Kerngeschäft
- Einhaltung von Haftungsanforderungen
- Im Wiederherstellungsfall stehen die Daten schnell auf dem lokalen Backup-Server bereit
- Im Katastrophenfall (Brand, Wasser, Diebstahl, etc.) stehen die Daten im Rechenzentrum bereit.

- Vermeidung von hohen Datenrettungs- und Installationskosten im Fehlerfall
- Einhaltung von gesetzlichen Bestimmungen zur Aufbewahrung von Daten
- Kostenkontrolle, fester monatlicher Preis für Datensicherung und Überwachung, keine weiteren Nebenkosten

Kontakt:

...iutax Steuer & Recht
Holger Fuchs
Ridlerstr. 35
80339 München
www.iutax.de

Branche: Steuerberater- und Rechtsanwaltssozietät

A.12 Ganzheitliches „gelebtes“ Schutzkonzept

Tobias Berens

TerraSana LIFE AG

Konzept

Ganzheitliches „gelebtes“ Schutzkonzept. Dazu zählen u.a.:

1. **Detailliertes strukturiertes Konzept zum Datenzugang („Need to know -Prinzip“)**
   - Definierter administrativer Prozess nach ITIL zur Einrichtung und Löschung von Usern
   - Definierter Prozess nach ITIL zur Verwaltung der Individuellen Zugangsrechte für jeden Mitarbeiter
   - Rollenbasierter Prozess der Ordnerfreigaben pro Mitarbeiter stellt sicher, dass nur auf die Daten zugegriffen werden kann, die für die konkrete Leistungserfüllung benötigt werden
   - Prozess nach ITIL zur regelmäßigen Überprüfung von Rollen und Rechten (laufend bei Änderung)
   - Richtlinien zur Komplexität (Güte) und Lebenszyklen von Kennwörtern (Beispiel Länge des Passwortes mind. 9 Zeichen, voller Zeichensatz, 6 Monate Gültigkeit, keine Wiederholung in 5 Wechselzyklen; die Einhaltung wird auch technisch erzwungen)
   - Aufbewahrung der handschriftlichen Daten nur unter Verschluss im Büro
2. **Sensibilisierung und Schulung der Mitarbeiter**
   - Jährliche Schulungen der Mitarbeiter zu IT-Sicherheit und Datenschutz.
   - Laufende Sensibilisierung der Mitarbeiter durch: Rundschreiben und Jour Fixes via Videokonferenz (ca. 1 x monatlich)
   - Sensibilisierung der Mitarbeiter durch die Geschäftsleitung
   - Individualschulung der Mitarbeiter (anwendungsspezifisch)
   - Im Rahmen der Koordinatoren-Ausbildung (Mitarbeiter vor Ort) eigener Ausbildungsteil IT-Sicherheit und Datenschutz BDSG Erklärung für jeden Mitarbeiter verpflichtend. Diese wird regelmäßig jährlich erneuert.
   - Gesonderte Schweigepflichterklärung für die mit Anamnese Daten in Kontakt kommenden Mitarbeiter
   - Unterzeichnete BDSG Erklärung für jeden Dritten, der zur Leistungserfüllung eingesetzt wird („Netzwerkpartner“)
   - Übermittlung von Daten nur nach individueller Schweigepflichtentbindung unserer Mitarbeiter vom Kunden, um mit Netzwerkpartnern Details kommunizieren zu können (Einzelbetreuung, Case-Management).
3. **Mobile Sicherheit**
   - Die Privatnutzung des (mobilen) Equipments ist explizit untersagt
   - Mitarbeiter beim Kunden können mobil auf definierte Dienste über VPN bei TerraSana LIFE zugreifen (vollständig entkoppelt von der Infrastruktur des Kunden)
   - Zur Datenübernahme dürfen nur zertifizierte USB-Sticks benutzt werden

Nutzen

Die TerraSana LIFE AG arbeitet insbesondere mit Großkunden zusammen, die höchste Sicherheitsstandards beim Umgang mit persönlichen Mitarbeiterdaten und Unternehmensdaten voraussetzen. Durch die Arbeit im Bereich Gesundheit unterliegt die TerraSana LIFE AG und deren Mitarbeiter darüber hinaus einer ähnlich strengen Verschwiegenheitspflicht wie z.B. Ärzte.

- Eine hohes Niveau in punkto IT-Sicherheit ist Voraussetzung für die Kundenbeziehung und ausschlaggebend für die Reputation im Markt.

- Der Umgang mit der Datensicherheit spiegelt wider, wie wir selbst gerne behandelt werden wollen, fehlende Datensicherheit wäre ein KO -Kriterium für unser Unternehmen.
- Wissen ist unser Kapital. In Jahren aufgebaute Wissensdatenanken sind die Basis unserer Arbeit und reduzieren das Risiko der Abhängigkeit von Einzelpersonen. Der umfassende Know-How-Schutz ist für unser Unternehmen existentiell und eine betriebswirtschaftliche Investition in die Zukunftssicherung des Unternehmens.
- Risikominimierung wg. Haftung (Konventionalstrafen, Bußgelder) und zum Schutz der Mitarbeiter

Kontakt:

TerraSana LIFE AG
Alexander Gmeiner
Ridlerstr. 35
83700 Rottach-Weißach
www.terrasanalife.de

Branche: Personalentwicklung in Verbindung mit betrieblichem Gesundheitsmanagement

A.13 IT-Sicherheitskonzept der Computer-L.A.N. GmbH

Oualid Nouri, Andree Schrimpf, Tina Heppenstiel, Michael Haeuser, Peter Dirksen, Florian Aff

Computer-L.A.N. GmbH

Konzept

Bei der Computer-L.A.N. GmbH gibt es eine niedergeschriebene Sicherheitsrichtlinie. Diese Richtlinie haben wir eingeführt, um den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) gerecht zu werden. Ziel war es, die Datensicherheit und die Verfügbarkeit der Daten und Systeme im Betrieb zu gewährleisten, ohne die Arbeitsabläufe zu behindern.

Sensibilisierung und Schulung der Mitarbeiter

Den Text der Sicherheitsrichtlinie geben wir jedem neuen Kollegen bei der Vertragsunterzeichnung und erläutern jeden einzelnen Punkt. Anschließend muss der Mitarbeiter unterschreiben, dass er die Richtlinie gelesen hat und sie einhalten wird. Das Dokument liegt auf unserem Server in einem Ordner, auf den jeder Mitarbeiter zugreifen kann.

Zugangskontrolle

Unsere Haustür und die Etagentüren sind mit Sicherheitsschlössern ausgestattet. Die Haustür ist grundsätzlich geschlossen. Besucher müssen sich über die Türsprechanlage anmelden. Sie werden dann vom Personal abgeholt und im Haus begleitet. Wenn der letzte Mitarbeiter auf einer Etage seinen Arbeitsplatz verlässt, verschließt er die betreffende Etagentür. Auch die Serverräume sind grundsätzlich verschlossen. Die Schlüssel für diese Räume verwaltet unser Administrator.

Netzwerk-Administration

Jeder Mitarbeiter bekommt mit Beginn der Firmenzugehörigkeit eine Benutzerkennung und ein Passwort. Damit meldet er sich an den Rechnern des Unternehmens an. Abhängig vom Arbeits- und Aufgabenbereich erhält er differenzierte Zugriffsrechte auf bestimmte Serververzeichnisse und Programme.
Die Systemeinstellungen in Windows haben wir so angepasst, dass jeder Kollege sein Passwort regelmäßig ändern muss. In den „Kennwort-Richtlinien“ ist festgelegt, wie ein neues Passwort aussehen darf (im Hinblick auf Länge und Form). Kollegen, die im „Home-Office“ arbeiten, können über individuelle, verschlüsselte VPN-Zugänge auf unser Netzwerk zugreifen. Der Zugang ist auf fest definierte Computersysteme beschränkt und funktioniert nur mit einem Passwort.

Zum Schutz des Unternehmensnetzwerkes nutzen wir eine Firewall. Die Computer werden durch Virenschutzsoftware und den Einsatz von Spam-Filtern geschützt.

Mobile Sicherheit

Alle Daten, die auf mobilen Datenträgern wie Notebooks, externen Festplatten oder USB-Sticks gespeichert sind, verschlüsseln wir mit einer kostenlosen Software. Um auf die Daten zuzugreifen, muss lediglich das Kennwort eingegeben werden, sodass der produktive Arbeitsablauf durch die Verschlüsselung nicht beeinträchtigt wird.

Datenschutz und Datensicherheit

Wenn ein Mitarbeiter seinen Arbeitsplatz verlässt, sperrt er seinen Computer. Arbeitsplätze mit Publikumsverkehr haben wir so eingerichtet, dass Dritte nicht auf den jeweiligen Monitor schauen können. Sensible, nicht mehr benötigte Daten löschen wir mithilfe spezieller Programme, damit die Daten nicht von Dritten wiederhergestellt werden können.
Zur Sicherung unserer Daten nutzen wir eine Datensicherungssoftware, mit der alle Server auf ein NAS-System (Netzwerkspeicher) gesichert werden. Um im Fall eines Datenverlusts (z. B. durch Einbruch oder Brand) die Verfügbarkeit der Daten zu gewährleisten, lagern wird die Daten des NAS-Systems täglich auf externe Medien aus. Diese Datenträger werden jeden Tag gewechselt. Die zuständigen Mitarbeiter nehmen sie nach Feierabend mit und bewahren sie außerhalb der Firma

auf.
Für die Rücksicherung im Katastrophenfall haben wir einen Notfallplan entworfen. Die Umsetzbarkeit des Plans üben wir regelmäßig ein.

Nutzen

Indem wir eine IT-Richtlinie formuliert und umgesetzt haben, beachten wir Vorschriften, die im Bundesdatenschutzgesetz (BDSG) festgelegt sind. Die Einhaltung des BDSG bedeutet auch eine Entlastung der Geschäftsführung.

Sensibilisierung und Schulung der Mitarbeiter

Neben der Sicherheit der eingesetzten Informationstechnologien konnten wir durch die korrekte Handhabung auch die Produktivität steigern. Nicht zuletzt durch die einfache Umsetzung ist die Akzeptanz der Mitarbeiter gegenüber den Richtlinien sehr hoch.

Zugangskontrolle

Durch die Absicherung der Hauszugänge und Etagentüren sorgen wir dafür, dass kein Unbefugter auf unsere IT-Infrastruktur zugreifen kann.

Netzwerk-Administration

Mit Hilfe der Firewall-Lösung schützen wir uns gegen unberechtigte Zugriffe von außen und vermindern das Risiko von Cyber-Spionage. Über die beinhaltete VPN-Funktionalität und kostenlose VPN-Software ist eine sichere Anbindung der Home-Office-Arbeitsplätze garantiert. So können wir flexible Arbeitszeit-Modelle nutzen.

Jeder Computer ist durch Benutzername und Kennwort geschützt. So stellen wir sicher, dass nur der betreffende Mitarbeiter auf die jeweiligen Daten zugreifen kann.

Mobile Sicherheit

Durch die Verschlüsselung von mobilen Geräten sorgen wir dafür, dass im Fall von Verlust oder Diebstahl Dritte keinen Zugriff auf sensible Daten bekommen. Da wir hierfür kostenlose Programme einsetzen, ist der Kosten-Nutzen-Faktor sehr hoch.

Datenschutz und Datensicherheit

Den Schutz von sensiblen Daten haben wir dadurch erhöht, dass wir die Arbeitsplätze entsprechend gestaltet haben und die Computer sperren, wenn ein Mitarbeiter seinen Arbeitsplatz verlässt.

Die Daten der Mitarbeiter sind durch die persönlichen Benutzer- und E-Mail-Konten geschützt. Wichtige Daten werden auf dem Server abgelegt und regelmäßig gesichert. Auf diese Weise erreichen wir, dass unsere Daten und Systeme dauerhaft sicher und verfügbar sind. Im Vergleich zu dem Schaden, der im Fall eines Datenverlustes entsteht, sind die Kosten für die Datensicherungssoftware und die benötigte Hardware marginal.

Personenbezogene Dokumente, die wir nicht mehr benötigen, löschen wir sicher, indem wir frei erhältliche Hilfsprogramme nutzen.

Produktivität

Anwendungen werden häufig aus Unkenntnis nicht richtig genutzt, so dass die Möglichkeiten der Software nicht vollständig ausgeschöpft werden. Durch die Schulungen konnten wir neben der Sicherheit auch unsere Produktivität erhöhen. Neuen Mitarbeiter erläutern wir neben dem sicheren Umgang mit E-Mails zum Beispiel auch, wie sie Microsoft Outlook im Arbeitsalltag effizient einsetzen.

Die integrierten Spam-Filter in der Firewall haben den Effekt, dass weniger unerwünschte E-Mails in den Posteingängen landen. Dadurch sparen wir wertvolle Arbeitszeit.

Fazit

Durch die Umsetzung unserer Richtlinie haben wir mehrfach profitiert: Zum einen haben wir viele Punkte des BDSG umgesetzt, zum anderen garantieren wir die Sicherheit und Verfügbarkeit aller unternehmensrelevanten Daten und Systeme. Unsere Arbeitsabläufe werden dadurch nicht behindert, die Kosten für spezielle Hard- und Software sind vergleichsweise gering.

Kostenübersicht:
Interner Arbeitsaufwand: 5 Tage à 8 Stunden = 1.800 Euro
Hardwarekosten (Firewall, NAS-System, externe Medien): ca. 2.700 Euro
Softwarekosten (Datensicherungssoftware für Server): 1.260 Euro
Gesamtkosten: 5.760 Euro

Kontakt:

Computer-L.A.N. GmbH
Andree Schrimpf, Tina Heppenstiel, Oulid Nouri, Michael Haeuser, Peter Dirksen, Florian Aff
Königstr. 42
36037 Fulda
www.computer-lan.de

Branche: IT- und Software-Systemhaus

A.14 Personalisiertes Server-Zugriffsmanagement

Simon Biela, Oliver Blum

kernpunkt GmbH

Konzept

Als Internetagentur warten wir Anwendungen und Webseiten, die auf Kundenservern gehostet werden. Als Zugriff wurde in der Vergangenheit pro Kunde meist ein Login (root) für alle Mitarbeiter in unserem Unternehmen zur Verfügung gestellt und genutzt. Um allen Mitarbeitern den Zugriff zu ermöglichen wurden die Passwörter und Zugänge in einer zentralen Datenbank verwaltet.

Aus IT-Sicherheitsperspektive war diese Situation unhaltbar. Alle Zugänge waren stets allen Mitarbeitern zugänglich. Ehemalige Mitarbeiter konnten auf Kundenserver zugreifen, da die Passwörter zwar in regelmäßigen Abständen, aber nicht mit jedem Mitarbeiterwechsel, verändert wurden. Da unsere Kunden auf Ihren Servern teils extrem sensible Daten verarbeiten und lagern musste eine einfach umzusetzende Alternativlösung geschaffen werden.

Das neue organisatorische Konzept sieht die Vergabe eines asynchronen Schlüsselpaars für jeden Mitarbeiter vor. Der öffentliche Teil des Schlüssels wird nun an zentraler Stelle von einem Agenturmanagementsystem bei den Profildaten des Mitarbeiters abgelegt. Den private Teil des Schlüssels führt der Mitarbeiter auf einem USB Stick am Schlüsselbund mit sich.

Innerhalb eines webbasierten Agenturmanagementsystems werden ohnehin bereits die einzelnen Mitarbeiter in Teams auf Projekte zugeordnet. Diese Zuordnung und eine zusätzliche Zuordnung von Servern zu Projekten macht sich das neue Konzept zu Nutze und gleicht die öffentlichen Schlüssel der auf ein Projekt zugelassenen Mitarbeiter mit den entsprechenden Kundenservern ab.

Hierzu werden die öffentlichen Schlüsselteile täglich an die Server gesendet oder von ihnen entfernt. Der Zugriff des Mitarbeiters auf den Server erfolgt dann mit Hilfe seines privaten Schlüssels.

Nutzen

Durch das neue organisatorische Konzept können nur noch Mitarbeiter auf Kundensysteme zugreifen, so lange sie Mitglied eines entsprechenden Projektteams sind. Ein neuer Zugriffsberechtigter kann mit wenigen Klicks hinzugefügt werden, verlässt ein Mitarbeiter das Projektteam oder das Unternehmen wird der Zugriff umgehend unterbunden.

Das umständliche Verwalten von Zugängen auf dem Server entfällt.

Die vom Kunden und Gesetzgeber geforderte Datenschutzkonformität, insbesondere die Nachvollziehbarkeit des personenbezogenen Zugrifft, ist gewährleistet.

Kontakt:

kernpunkt GmbH
Simon Biela, Oliver Blum
Oskar-Jäger-Strasse 170
50825 Köln
www.kernpunkt.de

Branche: Internetagentur für Beratung, Kreation und Realisierung von Intranet- und Internet-Projekten

A.15 Sensibilisierungsmaßnahme

Markus Stäudinger

Maschinenfabrik Gustav Eirich GmbH & Co KG

Konzept

Gemäß dem Grundsatz 'Sicherheit fängt im Kopf an' wurde das Konzept nicht auf technische, sondern auf menschliche Maßnahmen ausgerichtet. Ziel war es neben dem richtigen Verhalten am Arbeitsplatz im Umgang mit Informationen auch im privaten Umfeld einen Mehrwehrt zu bieten.

Anhand einer Fragebogenaktion und proaktiven Angriffen wurden der momentane Wissenstand und die Verhaltensweisen ermittelt. Diese Kampagne wurde erneut zum Anlass genommen, die internen Richtlinien zu überarbeiten und neu zu vermitteln.

Inhalte der Kampagne (Auszug):

- Erkennen von Pishing versuchen
- Umgang mit Informationen auf Dienstreisen
- Erkennen von Social Engineering Vorfällen
- Vermitteln der internen Richtlinien
- Klassifizierung von Informationen
- Das richtige Verhalten gegenüber Besuchern

Die komplette Maßnahme wurde Anhand von Schulungen/Workshops durchgeführt an der jeder Mitarbeiter teilnehmen soll.

Da das Sicherheitsverhalten vorgelebt werden soll, erfolgt die Durchführung in drei Stufen:

1. Führungskreis, d.h. Geschäftsführung incl. aller Entscheider. Hier wurde zusätzlich Herr Opfermann vom Landesamt für Verfassungsschutz gehört und von Dr. Andreas Gabriel der Uni Würzburg Live-Hacking durchgeführt.
2. Meister in der Produktion. Hier wurde Dr. Andreas Gabriel mit Live-Hacking aktiv
3. Mitarbeiter am Standort

Um das Ganze zu unterstützen wurde ein Awareness-Folder aufgelegt und zusätzlich eine kleine Sammlung von Give-Aways die witzig/provokant, und zugleich nützlich sind. Auch diese Sammlung wurde auf den privaten Mehrwert ausgelegt.

Die Nachhaltigkeit wird durch fortlaufende kleiner Aktionen auf dem Firmengelände, kleinere Gewinnspiele, Fragebogenaktionen und Newsletter sichergestellt.

Nutzen

Information ist das wertvollste Gut in jedem Unternehmen. Der Ausfall von Systemen und das Fehlverhalten von Mitarbeitern zur Verarbeitung von Information bedeuten einen finanziellen Schaden und können neben monetären Nachteilen auch zu Verlust von Image, Vertrauen und Reputation führen.

Gleichzeitig wird der Schutz von Informationen für jedes Unternehmen zu einer wachsenden Herausforderung, weil sich Technologien, Bedrohungen und Risiken ständig und schnell verändern. Folgender Nutzen wird erwartet:

- Zukunftssicherung durch bewussten und sicheren Umgang mit Informationen
- Sicherstellung der Verantwortung der einzelnen Mitarbeiter
- Bewusstseinssteigerung bei den Mitarbeitern
- Rechtzeitige Erkennung von Gefahren und das richtige Handeln danach
- Steigerung der Präsenz des Sicherheitsmanagements
- Nachhaltige Verhaltensänderungen der Mitarbeiter im Umgang mit sensiblen Informationen
- Signalwirkung gegenüber Kunden und Lieferanten

Kontakt:

Maschienfabrik Gustav Eirich GmbH & Co KG
Markus Stäudinger
Walldürnerstrasse 50
74736 Hardheim
www.eirich.de

Branche: Mischtechnik, Granuliertechnik, Trocknungstechnik, Feinmahltechnik

A.16 Sichere Organisation und Betrieb einer Informationsplattform für Kunden

Peter Erat, Dr. Janko Schildt

Emperra GmbH

Konzept

Wir betreiben ein eigenentwickeltes System (ESYSTA) zum automatisierten telemedizinischen Monitoring von Diabetes mellitus-Patienten. Hierzu gehören neben unserem Online-Portal das ESYSTA-Pen oder –Blutzuckermessgerät sowie ggfs. die ESYSTA-App für Smartphones. Zur umfassenden Betreuung der Patienten betreiben wir eine Informationsplattform, die sowohl telefonisch als auch per Email angesprochen werden kann. Sie ist die zentrale Anlauf- und Vermittlungsstelle für Anfragen zu technischem Support für alle Komponenten des ESYSTA-Systems, zur Ernährung (Diät) und medizinischen Fragen.

Dies erfordert einen sensiblen und differenzierten Umgang mit den anfallenden Daten. Sie müssen nach Sensitivität und Fachlichkeit bewertet und nach Art (Telefon oder Email) und Intention (technisch, ernährungsberatend, medizinisch) der Anfrage prozessiert werden (Datenverarbeitung, Speicherung.)

Maßnahmen:

- Innerhalb der Emperra GmbH wurde ein von den übrigen Räumlichkeiten separierter, abschließbarer Arbeitsplatz geschaffen.
- Organisatorisch wird der Raum durch Arbeitsanweisungen und Prozessanweisungen administrativ von der übrigen Infrastruktur getrennt.
- Vertretungsregelungen sind gemäß der Verfügbarkeitsanforderungen definiert.
- Persistente Aufzeichnungen von Patientendaten sind generell untersagt.
- Die Prozesse fordern unter anderem, dass im Falle
    a. einer medizinischen Anfrage nur mir einem Hinweis auf kompetente Stellen geantwortet wird. Es findet keine medizinische Beratung durch uns statt. Eine eingegangene Email wird sicher gelöscht, der Inhalt eines Telefonats wird nicht protokolliert.
    b. einer Anfrage zur Ernährungsberatung per Email nur mit einer allgemeinen Information und einem Hinweis auf unser Partnerinstitut zur Ernährungsberatung beantwortet wird, ein Telefonanruf kann hingegen dorthin weitervermittelt werden.
    c. einer technischen Supportanfrage oder Reklamation ggfs. eine Weitergabe der zur Bearbeitung unbedingt notwendigen Sozialdaten an unsere externen Partner bzw. unser Warenwirtschaftssystem stattfinden kann.
- Mit unseren externen Partnern sind konkrete Verfahren zur sicheren Datenübertragung vereinbart. Die Vertraulichkeit und der den Daten zukommende Schutzbedarf wurde mit der Datenschutzbeauftragten abgestimmt und über Zusatzverträge mit abgesichert.
- Die Mitarbeiter werden regelmäßig auf die sichere Durchführung der Prozesse geschult und dahingehend sensibilisiert, dass Sicherheit auch gelebt wird.
- Die Einhaltung der Maßnahmen wird durch unser Sicherheits- und Qualitätsmanagement und die Datenschutzbeauftragte laufend überprüft.

Die Emperra GmbH E-Health Technologies befindet sich im Auditierungsprozess zur Konstitution eines ISMS auf der Basis von IT-Grundschutz. Das angestrebte Sicherheitsniveau wird in der IT-Sicherheitsleitlinie definiert. Die daraus abgeleiteten Richtlinien und Rahmendokumente stellen sicher, dass das Sicherheitskonzept alle Ebenen der Emperra GmbH mit einbezieht.

Nutzen

Die umgesetzten organisatorischen Maßnahmen

- Sind Voraussetzung für das Funktionieren des Geschäftsmodells

- Stellen sicher, dass gesetzliche Regelungen bzgl. des Datenschutzes nachprüfbar eingehalten werden,
- Stellen sicher, dass vertragliche Regelungen mit Partnern insbesondere aus dem medizinischen Bereich nachprüfbar eingehalten werden,
- Schaffen hohe Akzeptanz bei Kunden und Partnern

Kontakt:

Emperra GmbH Potsdam
Peter Erat, Dr. Janko Schildt
Friedrich-Ebert-Straße 33
14469 Potsdam
www.emperra.com

Branche: Medizintechnik und Dienstleistung

A.17 Sicherheitsanalyse anhand kritischer Geschäftsprozesse

Volker Lübbers

Hamburger Logistik Institut GmbH

Konzept

Die Sicherheitsanalyse der IT-Infrastruktur wurde nach einem Verfahren durchgeführt, dass aus dem Standard 100-2 des IT-Grundschutz vom BSI mit der Zielsetzung entwickelt wurde, besser für KMU anwendbar zu sein. Zu diesem Zweck ist u.a. der Geltungsbereich des ISMS auf die geschäftskritischen Geschäftsprozesse beschränkt worden.

Die Geschäftsprozesse wurden in zwei aufeinanderfolgenden Phasen herausgearbeitet.

1. Phase: Erstellen einer Auflistung aller Geschäftsprozesse

Die Geschäftsprozesse wurden in einer qualitativen moderierten Gruppenbefragung erfasst. Ergebnis der Befragung ist eine tabellarische Auflistung, in der die Geschäftsprozesse, die wesentlichen Aktivitäten innerhalb eines einzelnen Geschäftsprozesses und die IT-Systeme, von denen diese Aktivitäten abhängen, enthalten sind.

2. Phase: Auf Basis der Liste aller Geschäftsprozesse wurden die geschäftskritischen Prozesse festgelegt.

Geschäftsprozesse gelten bei unserem Vorgehen als geschäftskritisch, wenn bereits ein Ausfall eines solchen Geschäftsprozesses von weniger als 24 Stunden einen geschäftskritischen Schaden für das Unternehmen bedeutet. Mit den Verantwortlichen wurde bestimmt, welche der erfassten Geschäftsprozesse nach dieser Definition geschäftskritisch sind. Die Ergebnisse wurden inklusive der Begründung dokumentiert.

Für eine bessere Übersicht bei der späteren Analyse der Geschäftsprozesse und deren Abhängigkeiten wurde zunächst ein vollständiger Netzplan erstellt. Dabei handelt es sich um eine grafische Übersicht der IT-Systeme, Netzwerkkomponenten und ihrer Verbindungen untereinander.

Ausgehend von der tabellarischen Auflistung aus der ersten Phase wurde in folgender Reihenfolge bestimmt, von welchen Objekten die geschäftskritischen Prozesse abhängen:

1. Geschäftskritischer Geschäftsprozess
2. Benötigte IT-Anwendungen
3. Zugehörige IT-Systeme
4. Zugehörige Kommunikationsverbindungen
5. Zugehörige Räume

Die Ergebnisse wurden in einer Zuordnungstabelle zusammengefasst, in der auch vermerkt ist, warum jeweils eine Abhängigkeit vorliegt.

Basierend auf den Ergebnissen der Analyse konnten aus den IT-Grundschutzkatalogen des BSI geeignete Maßnahmen vorgeschlagen werden.

Nutzen

Das Unternehmen hat nun neben einem vollständigen Netzplan eine Übersicht seiner kritischen Geschäftsprozesse, kennt die Abhängigkeiten dieser Prozesse von IT-Anwendungen, IT-Systemen, Kommunikationsverbindungen und Räumlichkeiten.

Zur Erreichung eines akzeptablen IT-Sicherheitsniveaus können nun geeignete Maßnahmen ausgewählt werden, wobei wirtschaftliche Aspekte und Ressourcenaspekte berücksichtigt werden können.

Kontakt:

Hamburger Logistik Institut GmbH
Volker Lübbers
Bredowstraße 20
22113 Hamburg
www.hli-consulting.de

Branche: Logistik Institut

A.18 Sicherheitszertifizierung

Mark Doerbeck

COMback GmbH

Konzept

Als Teil der grundsätzlich datenzentrischen und sicherheitszentrischen Betrachtungsweise in unserer kleinen IT-Security-Unternehmensgruppe haben wir vor ca.5 Jahren die Entscheidung getroffen, die operative Tochtergesellschaft der Gruppe, die COMback GmbH, mit allen ihren Geschäftsprozessen nach ISO 27001 auf Basis BSI Grundschutz für hohen und sehr hohen Schutzbedarf zertifizieren zu lassen.

Wir haben dies trotz anfänglich hoch erscheinender Kosten als notwendig erachtet, weil wir glauben, dass nur wer konsequent Sicherheit lebt auch langfristig von der Vermarktung seiner Sicherheits-Dienstleistungen leben kann.

Nach mehr als einem Jahr Planungs-, Vorbereitungs-und Umsetzungszeit haben wir durch stringentes Optimieren und vor allem Dokumentieren aller Prozesse im Unternehmen im Frühsommer 2008 die Zertifizierung erhalten. In den folgenden drei Jahren wurden die erforderlichen jährlichen Überprüfungs-Audits planmäßig durchgeführt. Die Arbeiten an den Prozessen und deren Dokumentation in den letzten 12 Monaten führten zu einer Rezertifizierung im Monat Juni 2012, wiederum für alle Unternehmensprozesse und - nach unserem Kenntnisstand - in diesem umfassenden Maß wiederum als einziges Unternehmen in Deutschland.

Von Anbeginn des Vorhabens waren alle Mitarbeiter des Unternehmens mit eingebunden. Durch konsequente Führung, jederzeit umfassende Information und offene Darstellung und Diskussion der Notwendigkeit der Maßnahme konnte ein ebenso durchgängiges und dauerhaftes Verständnis, wie die selbst nach 5 Jahren ungebrochene Bereitschaft aller Kolleginnen und Kollegen zu engagierter Mitarbeit erreicht werden.

Nutzen

Eine ausschließlich auf Zahlen basierende Kosten-/Nutzenanalyse erscheint ebenso wenig sinnvoll wie über den Wert einer Risiko-Lebensversicherung zu diskutieren. Der Aufwand ist zweifellos hoch. Das Zertifizierungs-Siegel ist jedoch nur ein -zwar reizvoller, aber nachgeordneter- Nebeneffekt.
Die ständige Beschäftigung aller Mitarbeiter mit den Strukturen und Prozessen des eigenen Unternehmens führt zu tiefen Erkenntnissen, zur Fähigkeit versteckte Schwachstellen zu erkennen, also "Betriebsblindheit" zu überwinden und dauerhaft zu vermeiden. Der Blick wird am eigenen Betrieb geschärft für Probleme der Kunden, die so schneller und effizienter gelöst werden können. Die Akzeptanz bei Kunden erhöht sich nachweislich und das Zugehörigkeitsgefühl der Mitarbeiter zu einem eingeschworenen Team steigt deutlich. Gerade aus unterschiedlichen Blickwinkeln entstehende kontroverse Diskussionen bringen das Unternehmen inhaltlich voran und stärken den Zusammenhalt weiter. Wir können die Frage nach Nutzen und Aufwand klar beantworten: Wir würden es jederzeit wieder tun!

Kontakt:

COMback GmbH
Mark Doerbeck
CITA/Jägerhaus
75394 Oberreichenbach
www.comback.de

Branche: Rechenzentrum, Backup, Recovery, Hochsicherheits-Housing/-Hosting, Consulting…

A.19 Verteilter Datenzugriff bei der Freiwilligen Feuerwehr Mössingen

Thomas Lauria

Freiwillige Feuerwehr Mössingen

Konzept

Die Freiwillige Feuerwehr Mössingen ist entsprechend der Ortsteile dezentral organisiert. In jedem Ortsteil gibt es eine Feuerwache als eigener Standort. Des Weiteren werden anfallende Aufgaben zum Teil auch vom heimischen PC der ehrenamtlichen Mitglieder wahrgenommen. Dabei liegen die Daten zentral auf einer NAS im Feuerwehrhaus des größten Ortsteils, im Folgenden "zentrales Feuerwehrhaus".

Auf diese Daten kann im zentralen Feuerwehrhaus per LAN und WLAN zugegriffen werden. Ein Zugang der weiteren Standorte (inkl. Heimische PCs) ist per VPN möglich. Die Daten gliedern sich in zwei Gruppen:

- "Öffentlich" für Mitglieder der Feuerwehr, z.B. Einsatz- & Übungsdokumentation, Einsatzunterlagen, etc. pp
- Führungsinformation, z.B. Personaldaten, Ausbildungsdaten, Lehrgangsanmeldungen, etc. pp.
- Diese Trennung ist auch dem Datenschutz geschuldet.

Im Einzelnen sieht das Datenzugriffskonzept vor, dass

- Die "öffentlichen" Daten zugreifbar sind sobald man sich im Intranet angemeldet hat (Benutzername, Passwort)
- Auf die Führungsdaten nur mit gesonderter Authentifizierung zugegriffen werden kann,

WLAN Zugriff nur bei Kenntnis der WPA Schlüssel und einer eingetragenen MAC Adresse möglich ist, dieser steht nur einer ausgewählten Personengruppe zur Verfügung.

- Zugriff von außen per VPN möglich ist - nach Aufbau der Verbindung findet man sich im Intranet wieder. Die Führungsinformationen sind nach wie vor per separatem Kennwort geschützt. Ein Zugriff per VPN ist nur bestimmten Funktionsträgern vorbehalten.
- die an der Einsatzstelle vor Ort benötigten Daten auf dem Rechner im Einsatzleitwagen (mobile Einsatzzentrale) gespiegelt sind. Zusätzlich wäre es im Notfall möglich, aus dem Einsatzleitwagen eine VPN Verbindung ins Feuerwehrhaus aufzubauen.

Weiterhin sieht unser Konzept Maßnahmen zur Sicherstellung der Datenverfügbarkeit vor. Dies sind:

- Datensicherung: momentan werden die Daten regelmäßig auf eine externe Festplatte gesichert. Aktuell werden andere Sicherungsmodelle evaluiert.
- Unterbrechungsfrei Stromversorgung: generell ist die gesamte Technik im zentralen Feuerwehrhaus mit einer kurzen Anlaufunterbrechung notstromversorgt. Aufgrund dieser Unterbrechung werden Einsatzleitrechner und der Datenserver mit einer zusätzlichen USV abgesichert.

Nutzen

Der Nutzen daraus: der räumlich getrennten Organisationsstruktur der Feuerwehr Mössingen - wie im Abschnitt Unternehmen beschrieben – wird Rechnung getragen. Zugriff auf besondere Daten (z.B. Personaldaten) ist nur bestimmten Personen gestattet. Die Sicherheit der Daten durch Sicherungskopien ist gewährleistet.

Kontakt:

Freiwillige Feuerwehr Mössingen
Thomas Lauria
Goethestraße 9
72116 Mössingen

www.feuerwehr-moessingen.de
Branche: Freiwillige Feuerwehr

B Danksagung

Die Entstehung dieses Trendpapiers ist vom Bundesministerium für Wirtschaft und Technologie im Rahmen des Projektes „KMU-Informationssicherheits-Awareness“, vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der Förderung des European Center for Security and Privacy by Design (EC SPRIDE, http://www.ec-spride.de, Förderkennzeichen 16BY1171), von CASED (www.cased.de) und von der Horst Görtz Stiftung unterstützt worden. Die Autoren danken den beiden Bundesministerien, der LOEWE Förderung des HMWK und der Horst Görtz Stiftung für diese Unterstützung. Weiter sprechen wir unseren Dank gegenüber der Task Force „IT-Sicherheit in der Wirtschaft“ aus.

Persönlich bedanken wir uns bei Frau Grauenhorst und Frau Reitz für die hilfreiche und unermüdliche Unterstützung.