

## bw digitronik. Ihr Partner für Informationssicherheit mit Köpfchen.



Informationssicherheit aus einer Hand: Technologie + Mensch + Organisation. Auf die Wirksamkeit jeglicher Sicherheitsmassnahmen kommt es an. Darin sind wir stark: Im Analysieren und Aufzeigen effizienter Massnahmen – mit Köpfchen, versteht sich.



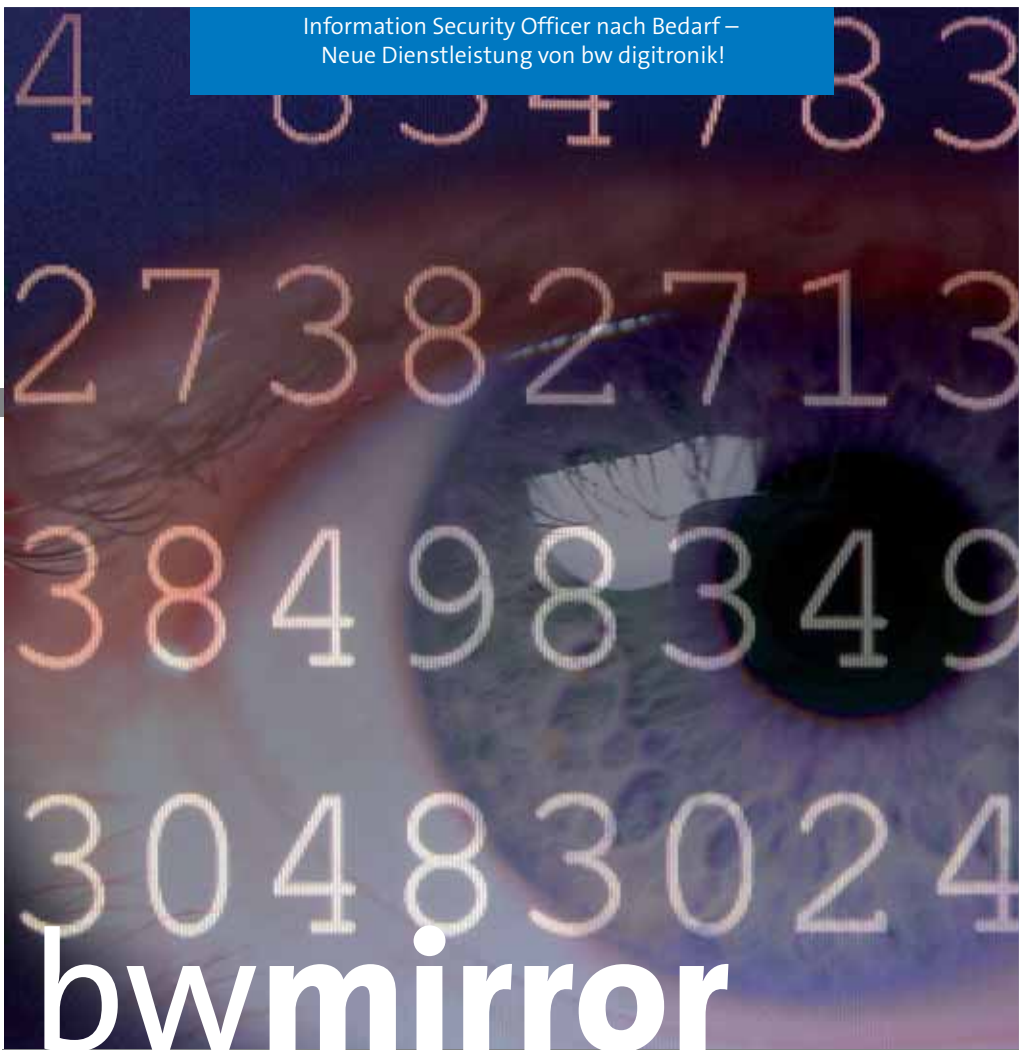
Hauptfunktionen	Kundennutzen	Einsatzbereich empfohlen
 E-SECURITY IS OUR MISSION	<ul style="list-style-type: none"> <li>- Information Security Officer auf Zeit</li> <li>- Policy Überprüfung und Erstellung</li> <li>- Security Konzepte und Beratung</li> <li>- Security Compliance Beratung</li> <li>- Security Audits nach GSH / BSI</li> <li>- Awareness Schulung &amp; Beratung</li> </ul>	<ul style="list-style-type: none"> <li>- Sicherheit umsetzen &amp; überprüfen</li> <li>- Klare Richtlinien für Sicherheit</li> <li>- Konzepte, die umsetzbar sind</li> <li>- Abgleich mit zu erfüllenden Normen</li> <li>- Überprüfung der internen Sicherheit</li> <li>- Sensibilisierte Mitarbeiter = Security</li> </ul>
 Sicherheit mit Kultur	<ul style="list-style-type: none"> <li>- Messen der Sicherheitskultur (Online)</li> <li>- Identifikation der Gefahren</li> <li>- Zeigt Awareness-Schwachstellen auf</li> <li>- Schafft Entscheidungsgrundlagen</li> <li>- Periodisches Benchmarking</li> <li>- Integrierbar in ISMS nach ISO 27001</li> </ul>	<ul style="list-style-type: none"> <li>- Überprüfung der Umsetzung der Sicherheitspolitik</li> <li>- Grundlage für Awareness-Schulung</li> <li>- Veränderung von Awareness messen</li> <li>- Wissensstand Mitarbeiter IT-Security</li> <li>- Erstellung &amp; Motivation Mitarbeiter</li> </ul>
	<ul style="list-style-type: none"> <li>- Data Loss Prevention</li> <li>- Foundstone Risk Assessment</li> <li>- Policy Enforcement</li> <li>- Anti-Spyware, Anti-Phishing/Pharming</li> <li>- Intrusion Prevention</li> <li>- SpamKiller und Content Filtering</li> <li>- Virenschutz für alle Ebenen</li> <li>- Management-Tool (ePO)</li> </ul>	<ul style="list-style-type: none"> <li>- Schutz vor (internem) Datenklau</li> <li>- Risiken definieren &amp; Schutz sichern</li> <li>- Richtliniendurchsetzung</li> <li>- Schutz vor Spyware, Adware ...</li> <li>- Hoher Schutz für Netzwerke / Hosts</li> <li>- Effiziente Abwehr der Spamflut</li> <li>- Schutz vor Viren, Würmern, Trojanern</li> <li>- Einfache Verwaltung &amp; Reporting</li> </ul>
	<ul style="list-style-type: none"> <li>- Managed Services für SMTP-Verkehr</li> <li>- SMTP &amp; WEB Appliance-Lösung</li> <li>- Content Filtering E-Mail-/Webverkehr</li> <li>- Spam-Filtering und -Verwaltung</li> <li>- URL-Blocking nach Kategorien</li> <li>- Benutzerspezifische Filterregeln</li> </ul>	<ul style="list-style-type: none"> <li>- Externer Gateway-Schutz</li> <li>- Kein Verlust von unerwünschtem Inhalt</li> <li>- Content Filtering vertraulicher Daten</li> <li>- Effiziente Abwehr der Spamflut</li> <li>- Erhöhte Produktivität der Mitarbeiter</li> <li>- Berücksichtigung einzelner User</li> </ul>
	<ul style="list-style-type: none"> <li>- Schutz für gemeinsame Files</li> <li>- Verschlüsselung für BlackBerry-Geräte</li> <li>- E-Mail-Verschlüsselung am Gateway</li> <li>- Desktop-Verschlüsselungslösungen: E-Mails, Files, Laufwerke, Notebooks</li> <li>- Schlüsselgenerierung und -verwaltung</li> <li>- Öffentliche Key-Server verfügbar</li> </ul>	<ul style="list-style-type: none"> <li>- Kein unbefugter Zugriff auf Daten</li> <li>- Geschützte Daten auf BlackBerrys</li> <li>- Vertraulicher E-Mail-Verkehr</li> <li>- Datensicherheit vertraulicher Infos</li> <li>- Datenschutz für mobile Rechner</li> <li>- Zentrales Key-Management</li> <li>- Automatische, regelbasierte E-Mail-Verschlüsselung am Gateway</li> </ul>
	<ul style="list-style-type: none"> <li>- Vulnerability Management</li> <li>- Automatisierte Patch-Verteilung</li> <li>- Multi-Plattformen-Unterstützung</li> <li>- Zentrales Management</li> <li>- Verteilte Anwendung</li> <li>- Überprüfung und Reporting</li> <li>- Patches durch Hersteller getestet</li> </ul>	<ul style="list-style-type: none"> <li>- Schwachstellen auffindig machen</li> <li>- Risikoverminderung durch rasche Beseitigung von Schwachstellen</li> <li>- Einhaltung von Sicherheitsregeln</li> <li>- Zentrale Kontrolle</li> <li>- Integration mit führenden Scannern</li> <li>- Reduzierte Kosten</li> </ul>
	<ul style="list-style-type: none"> <li>- Device Control (Sticks, Laufwerke ...)</li> <li>- Application Control (Software)</li> <li>- Zentrales Management</li> <li>- White-Listing-Methode</li> </ul>	<ul style="list-style-type: none"> <li>- Nur definierte Devices im Einsatz</li> <li>- Nur definierte Software im Einsatz</li> <li>- Schutz vor unerlaubter Software</li> <li>- Durchsetzen zentraler Richtlinien</li> <li>- Hoher Schutz, gute Kontrolle</li> <li>- Einfache Handhabung/Bedienung</li> </ul>
	<ul style="list-style-type: none"> <li>- Continuous Data Protection</li> <li>- Gateway Mail-Filtering (SMTP)</li> <li>- SSL-VPN Appliances</li> <li>- Firewall Appliances mit VPN</li> <li>- Secure Wireless</li> <li>- Total Secure Enterprise</li> <li>- Content Filtering</li> </ul>	<ul style="list-style-type: none"> <li>- Kontinuierliche Datensicherung</li> <li>- Schutz vor unerwünschtem Inhalt</li> <li>- Sichere Remote-Verbindungen</li> <li>- Zugriffsschutz und -kontrolle</li> <li>- Hackerschutz bei Angriffen</li> <li>- Schutz vor DoS-Attacken</li> <li>- Einfache Konfiguration</li> </ul>

## bw digitronik

E-SECURITY IS OUR MISSION

bw digitronik ag, Strickstrasse 15, CH-8610 Uster, Telefon +41 44 905 48 48, www.bwdigitronik.ch, info@bwdigitronik.ch

Information Security Officer nach Bedarf –  
Neue Dienstleistung von bw digitronik!



# bwmirror

InfoMagazin bw digitronik 2/07

Erhöhung der Informationssicherheit:  
Der Security Officer hilft.

Kritische Informationen vor neugierigen Blicken  
unberechtigter Dritter schützen.



## bw digitronik für Ihre Sicherheit!

Informationssicherheit gewinnt immer mehr Bedeutung in Unternehmen. In Umfragen wird gefordert: «CISOs gehören in die Unternehmensleitung!».

Um Führungskräfte und Sicherheitsverantwortliche besser in ihren wichtigen Aufgaben zu unterstützen, bietet bw digitronik weitere Dienstleistungen in den Bereichen Security Consulting und Awareness an. Denn um umfassende Sicherheit zu gewährleisten, sind nebst marktführenden Technologien auch organisatorische Massnahmen, wie verständliche und umsetzbare Policies, Notfall-Szenarien etc., wichtig. Besondere Aufmerksamkeit verdient dabei der Faktor Mensch. Studien decken immer wieder auf, dass gewiefte Hacker versuchen, den User mit immer raffinierteren Taktiken zu täuschen.

Professor Clive Hollin meint in einem aktuellen Bericht dazu: «Wenn die Botschaft ausreichend überzeugend ist und auf eine kritische Kombination von situativen und persönlichen Faktoren trifft, dann fallen die meisten Menschen darauf herein. Das gilt für erfahrene und unerfahrene Computerbenutzer gleichermaßen.»

Wir von bw digitronik unterstützen Sie dabei, ein umfassendes, unternehmensspezifisches Informations-Sicherheitskonzept zu

erstellen, welches die organisatorischen Massnahmen, den Menschen und die Technologie berücksichtigt.

bw digitronik für Ihre Informationssicherheit!

Herzlichst

*M. Viselka*

Martin Viselka  
Chief Executive Officer

## bw digitronik

E - SECURITY IS OUR MISSION

bw digitronik ag

CH-8610 Uster

Telefon +41 44 905 48 48

www.bwdigitronik.ch

Es gilt heute als allgemein akzeptiert, dass Informationen für eine Unternehmung einen der wichtigsten und damit am schützenswertesten Vermögenswerte darstellen. Informationen schützen? Da stellt sich gleich die Frage: Welche Informationen sollen geschützt werden?

## Erhöhung der Informationssicherheit: Der Security Officer hilft.

Zum oben Gesagten kommt noch erschwerend hinzu, dass es in einem Unternehmen sehr viele Informationen gibt. Diese können an ebenso vielen unterschiedlichen Orten liegen. Auf den ersten Blick scheint es fast unmöglich, in einer solchen Umgebung für den Schutz der so wichtigen Informationen zu sorgen. Doch mit einem systematischen Vorgehen kann auch diese Herausforderung gemeistert werden.

### Mit System zum Erfolg

Da Informationen sowohl auf IT-Systemen als auch auf Papier und in den Köpfen der Mitarbeiter existieren, wäre es dem Ziel nicht dienlich, sich nur auf technische Lösungen zu konzentrieren. Will man für die eigene Unternehmung ein angemessenes Informations-Sicherheitsniveau erreichen, muss mit System vorgegangen werden. Eine solche Vorgehensweise muss einen ganzheitlichen Ansatz verfolgen und neben technischen auch organisatorische und menschliche Faktoren einbeziehen. Dieses Vorgehen mit System wird auch als «Informations-Sicherheits-Management-System» (ISMS) bezeichnet und hat sich in der Praxis als sehr hilfreich erwiesen.

### Schritte zu einem eigenen ISMS

Das bis hierhin Gesagte ist ja schön und recht, doch welche konkreten Schritte beinhaltet ein solches «systematisches Vorgehen»?

Eine der wichtigsten Voraussetzungen für einen ganzheitlichen Schutz von Informationen ist, dass die Geschäftsleitung sich ihrer Verantwortung für Informationssicherheit bewusst ist und die anzustrebenden Sicherheitsziele unterstützt. Mit gutem Vorbild vorangehend, sollte die Geschäftsleitung einen entsprechenden Prozess

anstossen, der bezüglich Informationssicherheit alle Bereiche der Unternehmung tangiert. Doch nur anstossen und vergessen führt bekanntlich nicht zum Ziel. **Damit Sicherheitsmassnahmen Erfolg haben können, müssen diese in einem kontinuierlichen Prozess immer wieder überprüft und verbessert werden.** Denn die Umwelt ist ständigen Veränderungen unterworfen und so auch die für eine Unternehmung möglichen Bedrohungen. Daher muss eine für jede Unternehmung angepasste Sicherheitsstrategie erarbeitet werden, an welcher sich alle zu orientieren haben. Doch wer soll all dies – neben der täglichen Arbeit – auch noch erledigen können? Das ist eine berechnete Frage, die differenziert betrachtet werden muss:

### Der (IT-)Security Officer

In grossen Organisationen wird von der Geschäftsleitung eine für alle Sicherheitsfragen verantwortliche Person bestimmt. Diese Person trägt in der Regel die Bezeichnung «(IT-)Security Officer» und ist dafür zuständig, geeignete Sicherheitsstrukturen und -prozesse aufzubauen und einzuführen. Da die Sicherheit einer Unternehmung vom Beitrag aller Mitarbeitenden abhängt, ist es wichtig, auch diese in den Sicherheitsprozess einzubeziehen. Dazu gehört, dass die Mitarbeitenden für sicherheitsrelevante Fragestellungen geschult und sensibilisiert werden. Gemäss dem deutschen Bundesamt für Sicherheit in der Informationstechnik können die Aufgaben eines (IT-)Security Officers wie folgt zusammengefasst werden:

Der (IT-)Security Officer:

- bereitet die Auffassung der Unternehmensleitung über Stellenwert der IT, anzustrebendes IT-Sicherheitsniveau und die unternehmensweiten IT-Sicherheitsziele vor, formuliert sie aus und führt eine Entscheidung herbei.
- berichtet der Unternehmensleitung über den Status quo zur IT-Sicherheit.
- berät die Unternehmensleitung zu Fragen der IT-Sicherheit.
- entwickelt und formuliert die IT-Sicherheitsleitlinie und holt danach die Zustimmung der Unternehmensleitung ein.
- gibt die abgestimmte IT-Sicherheitsleitlinie allen betroffenen Mitarbeitern des Unternehmens bekannt.
- erlässt Richtlinien und Regelungen, auf welche Weise IT-Sicherheit im Unternehmen erreicht werden soll.
- unterstützt die Anwendung des IT-Grundschutzes und die Durchführung von Risikoanalysen zur Erstellung des IT-Sicherheitskonzeptes.
- koordiniert die IT-Sicherheitsziele mit den Unternehmenszielen zum IT-Einsatz und stimmt sie mit den IT-Strategien der einzelnen Unternehmensbereiche ab.
- legt die Aufgaben für IT-Sicherheit für den nachgeordneten Bereich fest.
- überprüft die erstellten IT-Sicherheitskonzepte auf Korrektheit und Nachvollziehbarkeit.
- bereitet die Unternehmensentscheidung über zu treffende, kostenträchtige IT-Sicherheitsmassnahmen vor und führt eine Entscheidung herbei.
- verwaltet die für IT-Sicherheit zur Verfügung

stehenden Ressourcen an Geld und Arbeitszeit.

- kontrolliert den Fortschritt der Realisierung von IT-Sicherheitsmassnahmen.
- koordiniert Kontrollen der Effektivität von IT-Sicherheitsmassnahmen im laufenden Betrieb.
- koordiniert Sensibilisierungs- und Schulungsmassnahmen zum Thema IT-Sicherheit.

All diese Aufgaben tragen signifikant zur Erhöhung und/oder Aufrechterhaltung der Sicherheit in einem Unternehmen bei. **Doch wer übernimmt diese wichtigen Aufgaben in kleineren und mittleren Organisationen? Auch dies ist eine berechnete Frage. Denn nicht alle Unternehmungen wollen oder können einen vollamtlichen Security Officer beschäftigen.** Hier trifft man häufig die Situation an, dass die Funktion des Security Officers in Personalunion mit dem IT-Leiter oder einem weiteren Angestellten ausgeübt wird. Diese sind aber in der Regel notorisch überlastet oder fühlen sich durch die steigenden gesetzlichen und regulatorischen Anforderungen im Bereich Informations-Sicherheit nicht genügend ausgerüstet.

### Security Officer Dienstleistung

Hier hilft die neue Dienstleistung von bw digitronik weiter: Falls die eigenen Personalressourcen beim Thema Informations-Sicherheit nicht genügen, stellen wir Ihnen unser Wissen gerne auf Abruf bereit – auch projektbezogen direkt bei Ihnen vor Ort. Ihre Vorteile: Sie beziehen die Leistungen nur dann, wenn Sie entsprechenden Bedarf haben.

Unsere Experten stehen bereit, Sie in Ihrem Tagesgeschäft bei security-relevanten Themen zu beraten. Können wir auch Sie unterstützen?

**Nehmen Sie mit uns Kontakt auf!**

**Zu wenig Zeit für Ihre Informationssicherheit? Wir bieten Ihnen die passende Dienstleistung:**

## Information Security Officer nach Bedarf.

- Policies erstellen
- Security umsetzen
- Security Projektbegleitung
- Beratung d. Managements

**bw digitronik: Ihr Partner für Informationssicherheit. 044 905 48 71**

13 Jahre IT-Security Erfahrung (seit 1994)

**Fallen Ihre User auch auf die perfiden Psycho-Tricks der Hacker rein?**

**Awareness Beratung & Schulung Sensibilisierung ...**

- des Managements
- der Mitarbeitenden

im Umgang mit den Gefahren des Informationszeitalters.



**bw digitronik: Ihr Partner für Informationssicherheit. 044 905 48 71**



In letzter Zeit ist immer häufiger zu hören, dass unternehmensinterne vertrauliche Daten in die Hände von unberechtigten Dritten gelangt sind. Solche Vorfälle sind zu einem Teil auf Unachtsamkeit von eigenen Mitarbeitern zurückzuführen und zum anderen Teil auf gezielte Angriffe – sei es von innen oder von aussen.

## Kritische Informationen vor neugierigen Blicken unberechtigter Dritter schützen.

So werden heute elektronische Konstruktionspläne in aller Selbstverständlichkeit von der Engineering-in die Fertigungsabteilung gesendet. Wie schnell kann es da geschehen, dass jemand aus Unachtsamkeit den falschen E-Mail-Verteiler erwischt und so vertrauliche Daten die geschützte Umgebung der Unternehmensmauern verlassen. Und was ist mit dem Entwicklungs-Mitarbeiter, der zu Hause weiterarbeiten will? Sind die Daten während dem Transport geschützt? Das Szenario vom verloren gegangenen USB-Stick (Laptop, CD-ROM etc.) mit wichtigen Unternehmensdaten kann in so einem Fall schnell traurige Realität werden.

### Weitreichende Auswirkungen

Abgesehen von finanziellen Verlusten, besteht die Gefahr des Imageschadens. Ein solcher kann unter Umständen sogar grössere finanzielle Auswirkungen haben als der direkte Schaden. Dies könnte z. B. der Fall sein, wenn Kunden oder Partner glauben, ihre Daten seien nicht mehr sicher genug aufbewahrt, und so zur Konkurrenz abwandern. Ein solcher Imageschaden kann sich auch auf die Beziehungen einer Unternehmung zu ihrer Hausbank auswirken. Als Stichwort sei hier «Basel II» genannt, welches den Umgang einer Unternehmung mit operationellen Risiken als Messgrösse zur Bestimmung der Kreditwürdigkeit und damit der Kredit-Zinshöhe heranzieht. Hat ein Betrieb seine operationellen (IT-)Risiken im Griff, wird er auch von tieferen Kredit-Zinsen profitieren können.

Wie wir sehen konnten, ist der potentielle wirtschaftliche Schaden, der durch den Verlust von Vertraulichkeit entstehen kann, sehr hoch. Es ist daher nicht plausibel, weshalb trotzdem auf entsprechende Sicherheitsmassnahmen verzichtet wird oder diese immer wieder aufgeschoben werden.

Doch angenommen, die Gefahr würde für die eigene Umgebung als relevant eingestuft und man möchte entsprechende organisatorische und technische Massnahmen einleiten: Worauf soll geachtet werden? Welche Möglichkeiten gibt es? Was sind die Vor- und Nachteile der unterschiedlichen Verfahren?

### Verschlüsselung und seine Formen

Um kritische Informationen vor den neugierigen Blicken Unberechtigter zu schützen, entwickelten schon die alten Ägypter entsprechende, einfache Verfahren. Die Kryptologie hat sich um einiges weiterentwickelt, und es stehen heute zum Schutz von vertraulichen Informationen unterschiedliche Verfahren zur Verfügung. Die einzelnen Verfahren zu beschreiben, würde den Rahmen dieses Textes sprengen. Doch je nach Anwendungsfall ist die eine oder andere Methode zu bevorzugen. So sollen in der Folge zwei Haupt-Anwendungsfälle für Verschlüsselung unterschieden werden:

- Eine einmal verschlüsselte Information soll an einer Stelle aufbewahrt werden, bis ein autorisierter Zugriff erfolgt. Hier geht es also um die Verschlüsselung von Datenträgern in all ihren Ausprägungen, wie z. B. Datei-, Verzeichnis-, Container- und Festplattenverschlüsselung.
- Eine Übertragung von kritischen Informationen über unsichere Netze: Ein potentieller Angreifer soll mit der abgefangenen Information nichts anfangen können. Ein konkreter Anwendungsfall ist hier die Verschlüsselung von E-Mails.

### Datenträger-Verschlüsselung

Oft wird beim Thema Datenträger-Verschlüsselung an mobile Geräte wie Notebooks oder USB-Sticks gedacht. Doch nicht nur auf diesen Geräten macht eine Datenverschlüsselung Sinn. Häufig besteht das Bedürfnis der Geschäftsleitung, ihre Sitzungsprotokolle, Finanzzahlen sowie weitere vertrauliche Dokumente vor den (neugierigen) Blicken der IT-



Administratoren zu schützen. Natürlich kann das Problem auch durch organisatorische Mittel eingedämmt werden. Doch ohne eine adäquate Verschlüsselungslösung besteht immer die Möglichkeit der Einsichtnahme in diese besonders schützenswerten Daten.

Folgende Tabelle zeigt die Vor- und Nachteile der verschiedenen Datenträger-Verschlüsselungsmethoden auf.

Verschlüsselungs-Methode	Vorteile	Nachteile
<b>Dateiverschlüsselung</b>	• Für einfache Anwendungsfälle geeignet: E-Mail-Anhänge, Passwort-Files	• Manuelle Interaktion ist fehleranfällig • Rückstände vertraulicher Dateien in temporären Verzeichnissen möglich
<b>Verzeichnisverschlüsselung</b> Gegenüber Dateiverschlüsselung zu bevorzugen	• Für Netzlaufwerke gut geeignet • Gruppen-Fähigkeit durch entspr. Produkte möglich • Backup & Restore problemlos • Admins können Daten nicht lesen und daher nicht verdächtigt werden • Kritische Verzeichnisse können mitverschlüsselt werden • Weniger fehleranfällig, da Verschlüsselung transparent im Hintergrund erfolgt • Fileserver muss nicht separat geschützt werden, da Ver- & Entschlüsselung auf Client des Users geschieht	• Rückstände vertraulicher Daten können im Page-File des OS, in Offline-Ordern oder im Slack-Space der Harddisk (alte Daten in nicht gefüllten Sektoren) liegen und gelesen werden • Genügte eher nicht den Anforderungen mobiler Endgeräte
<b>Festplattenverschlüsselung</b> Zu bevorzugende Lösung, da verglichen mit Datei- & Verzeichnis-Verschlüsselung am sichersten	• Keine Angriffsfläche, da ganze HD verschlüsselt wird • Vollkommen transparente Ver- & Entschlüsselung • Mit Pre-Boot Authentication kombinierbar: OS wird erst gebootet, wenn Passwort/PIN richtig sind • Geringer Ressourcen-Verbrauch • Harddisks mit hochsensiblen Daten müssen nicht physisch zerstört werden	• Keine bekannt

Gleichgültig für welche am Markt erhältliche Lösung man sich entscheidet, auf folgende Anforderungen sollte man Wert legen:

- Anerkannte Verschlüsselungsverfahren
- Transparente Verschlüsselung im Hintergrund
- Beeinträchtigt nicht Arbeitsabläufe
- Zentrale Administration und Schlüsselverwaltung
- Einfache und skalierbare Unterstützung von Benutzergruppen
- Anbindung an gängige Directory Systeme (z. B. Microsoft Active Directory)
- Vier-Augen-Prinzip: Trennung von System- und Sicherheitsadministration
- Unterstützung von Smartcards und Tokens
- Zusammenarbeit mit anderen im Unternehmen

- eingesetzten Lösungen wie Backup, Imaging-Tools und Antiviren-Tools
- Nutzung von Synergien mit einer E-Mail-Verschlüsselungs-Lösung

Gerade der letzte Punkt schliesst den Kreis wieder und bringt uns zum Fall, wo vertrauliche Informationen über unsichere Netze übertragen werden müssen.

### E-Mail-Verschlüsselung

Bei der Übertragung von E-Mails über das Internet durchlaufen diese auf ihrem Weg zum Ziel diverse Zwischenstationen: Server, auf denen die Nachrichten kurzfristig im Speicher oder auf der Harddisk zwischengespeichert werden. Dies ist auch der Punkt, an dem aktiv in die Nachrichtenübertragung eingegriffen und die vertrauliche Information eingesehen werden kann. So könnte man z.B. mit einem Skript automatisch alle Nachrichten filtern, welche eine Kreditkarten-Nummer beinhalten. Zudem kann eine E-Mail-Nachricht auch verändert und weitergeleitet werden.

Um diesem Problem zu begegnen, haben sich zwei Standards etabliert: PGP und S/MIME. Diese sind zueinander nicht kompatibel, aber es gibt Lösungen, welche mit beiden Standards umgehen können.

**S/MIME** steht für «Secure Multipurpose Internet Message Extensions» und wird von den meisten modernen Mailclients unterstützt. Für den Betrieb sind digitale Zertifikate nach dem X.509v3 Standard nötig.

**PGP** steht für «Pretty Good Privacy» und ist die am meisten verbreitete Verschlüsselungs-Lösung. Sie basiert im Wesentlichen auf dem Prinzip des «Web of Trust», unterstützt aber auch digitale Zertifikate. PGP hat sich zu einem Quasi-Standard entwickelt und wird daher von praktisch allen E-Mail-Lösungen unterstützt.

**Durch Beratung zu einem erfolgreichen Projekt**  
Können wir Sie bei den Themen Verschlüsselung von E-Mails und Datenträgern unterstützen? Nehmen Sie mit uns Kontakt auf: Unsere Experten stehen Ihnen gerne zur Verfügung.



## Sanctuary Device Control



Uneingeschränkte Kontrolle über alle mobilen Medien und Endpunktgeräte sowie den gesamten Port-Zugriff.



Application Control  
Lückenloser Schutz vor Malware und unerwünschten Anwendungen.

**JETZT kostenlos TESTEN**  
**044 905 48 50**

**Verschlüsselungslösung mit zentralem Management. Die PGP Encryption Plattform bietet umfassenden Schutz für Unternehmensdaten:**

- E-Mail-Sicherheit
- Datei- & Festplattensicherheit
- Sichere Datenübertragung
- Storage-Sicherheit
- Geschützte Speichermedien
- Sichereres Instant Messaging

**bw digitronik berät Sie sicher und kompetent bei Verschlüsselungsprojekten.**  
**044 905 48 50**



## Kuhn Rikon AG – Seit 10 Jahren gut beraten wenns um Informationssicherheit geht.

### Netzwerk

- 6 Server, 79 Desktops, 8 mobile Rechner  
- Tochtergesellschaften sind autonom organisiert

### Sicherheitslösungen von bw digitronik

- Viren- und Spywareschutz: McAfee AVD  
- Security Management: McAfee ePO  
- Lokaler Support für McAfee:  
bw digitronik bwPLUS  
- Firewall/Gateway/Content Filter:  
SonicWALL TZ 170  
- Remote-Kommunikation: SonicWALL SSL-VPN  
- Patchmanagement: PatchLink Update  
- Beratung Informationssicherheit:  
bw digitronik

### Partnerschaft mit bw digitronik

- seit über 10 Jahren

### Background

Die Kuhn Rikon AG ist ein Familienunternehmen mit Hauptsitz in Rikon/Schweiz und mit Tochtergesellschaften in Grossbritannien, Spanien und den USA. Ein Verkaufsbüro in Singapur betreut die Kunden in Asien. Kuhn Rikon AG entwickelt, produziert und vertreibt qualitativ hochwertiges Kochgeschirr und Zubehör, welches gesundes und effizientes Kochen ermöglicht. Dank enger Zusammenarbeit mit Konsumenten, Kochschulen und Forschungsinstituten erfüllt das umfassende Kochgeschirr- und Küchenhelferangebot auch die Wünsche und Anforderungen der Partner im Handel.

### 10 Jahre Partnerschaft mit bw digitronik

Die Kuhn Rikon AG partnern im Bereich Informationssicherheit seit über 10 Jahren mit bw digitronik. Marcel Stäubli, seit über sieben Jahren Leiter Informatik, hatte schon bei seinem ehemaligen Arbeitgeber mit bw digitronik zu tun. Schon damals hat er gute Erfahrungen gemacht und

hat die Partnerschaft auch bei Kuhn Rikon AG weitergeführt. Marcel Stäubli beschreibt die Zusammenarbeit so: «Ich schätze es sehr, dass ich über die Jahre immer mit dem gleichen Ansprechpartner (Patrik Spiess) zu tun hatte. Er kennt unser Netzwerk und die Systeme und kann entsprechend schnell eine passende Lösung vorschlagen.» Weitere Pluspunkte sind die raschen Reaktionszeiten bei Supportanfragen und die technische Kompetenz, welche zur schnellen Problembehebung beigetragen hat. Vorteilhaft findet Marcel Stäubli auch die lokale Nähe: «So ist in kurzer Zeit jemand vor Ort und man kann auch in Randstunden weiterhelfen.» Auch das Lösungsportfolio von bw digitronik ist ihm sympathisch. Mit den bisher eingesetzten Technologien von marktführenden Herstellern ist Marcel Stäubli sehr zufrieden.

### IT-Sicherheitslösungen im Einsatz

Als umfassender Viren- und Spyware-Schutz ist bei Kuhn Rikon AG seit mehr als zehn Jahren McAfee im Einsatz. Auf Empfehlung von bw digitronik wurde für das Management der McAfee-Lösung das Verwaltungstool ePolicy Orchestrator installiert. «Mit dieser Lösung sind wir in den letzten Jahren sehr gut gefahren. Wir haben keinen einzigen Virus eingefangen», freut sich Marcel Stäubli. Dank dem Verwaltungstool ist einerseits eine genaue Überwachung der Aktivitäten möglich. Andererseits helfen die Reports dem Management nachzuvollziehen, vor welchen Bedrohungen ihr Unternehmen durch McAfee geschützt wurde. Als Gatewayschutz mit Content-Filter setzt Kuhn Rikon AG auf SonicWALL Appliances. Bisher haben sie sehr gute Erfahrungen gemacht und hatten noch keinen Hardware-Ausfall zu beklagen: «Die SonicWALL, sie läuft einfach und schickt Logs», erklärt Marcel Stäubli. Seit einigen Monaten wurde

für die sichere Remote-Kommunikation eine SonicWALL SSL-VPN Appliance ins Netzwerk eingebunden. Diese sei einfach zu bedienen, Benutzer können problemlos hinzugefügt werden und auch die Berechtigungen sind schnell definiert. Marcel Stäubli: «Ich habe sehr wenig Aufwand mit diesem Gerät.» Beim Patchmanagement setzt Kuhn Rikon AG auf die marktführende Lösung von PatchLink. Die Verteilung der Patches funktioniert einwandfrei und die Netzwerkbelastung ist gering.

### Blick in die Zukunft

Beim Gedanken an die Zukunft kommt Marcel Stäubli folgender Satz als erster über die Lippen: «Ich hoffe, dass Herr Spiess möglichst lange bleibt.» Er wünscht sich weiter, dass die gute Qualität der Betreuung und Beratung weiterhin bestehen bleibt – ob bei konzeptionellen oder support-technischen Fragen. Solange dies so bleibt, sieht er keinen Anlass, den Partner zu wechseln. Also dann, auf weitere zehn Jahre.



Marcel Stäubli, Leiter Informatik

## bw digitronik ganzheitlicher Ansatz: Organisation + Mensch + Technologie.



bw digitronik, seit 1994 in der Informations-sicherheit tätig, gehört zu den Schweizer Pionieren auf diesem Gebiet. Als Grundlage für die Security Consulting- und Awareness-Konzepte dienen die erprobten und international anerkannten «Best Practices» der Informationssicherheit wie das Grundschutzhandbuch (GSH/BSI) und der ISO-Standard 27001. Auf dieser Basis hat bw digitronik ihren Ansatz für ganzheitliche Unternehmens-sicherheit entwickelt: Informationssicherheit = **Organisation + Mensch + Technologie.**

**Organisation:** Bevor mit Informationssicherheit begonnen werden kann, muss das Management eine IT Governance aus den Unternehmenszielen ableiten. Auf der Basis dieses Dokuments kann erst eine sinnvolle Security Policy definiert werden. Folgende Punkte müssen darin geklärt werden: a) Definition der Computer-Ethik (Code of Behavior), b) Definition der Führungs- und Organisationsstruktur, c) Klassifizierung von Vermögenswerten bzgl. Vertraulichkeit, Integrität und Verfügbarkeit, d) Definition des Risiko- und Informationsmanagements (inkl. Reporting und Monitoring). Weitere Überlegungen betreffen die Einbindung der HR-Abteilung, um die Arbeitsverträge mit der Security Policy abzustimmen und um die Ausbildung der Mitarbeitenden im Bereich IT und Informationssicherheit zu fördern.

**Mensch:** Der Mensch ist ein sehr wichtiger Faktor in der Informationssicherheit. Er sollte die Security Policy verstehen und in seinem Arbeitsalltag umsetzen können. Er muss in der Lage sein, kritische Situationen als solche wahrzunehmen und entsprechend der Richtlinie zu handeln. Er sollte wissen, welche verantwortlichen Personen innerhalb des Unternehmens zu benachrichtigen sind, wenn etwas Sicherheitsrelevantes passiert. Darum ist es wichtig, dass vom Management bis zum einfachen Mitarbeiter alle sensibilisiert werden im Umgang mit der IT-Infrastruktur und besonders mit den Regeln aus der Security Policy. Je sensibilisierter der Mensch ist, desto höher ist die Informationssicherheit im Unternehmen. An dieser Stelle ist auch die Führungsethik zu beachten. Denn Führungskräfte, die nicht mit gutem Vorbild vorangehen, haben es schwer, von ihren Mitarbeitenden die Einhaltung der Security Policy einzufordern.

**Technologie:** Welche Sicherheits-Technologien notwendig sind, um die eigenen Vermögenswerte zu schützen, hängt von der Security Policy und der Risikobereitschaft des Unternehmens ab. Weiter kommt es darauf an, welchen nationalen oder internationalen Gesetzen und Regularien die entsprechende Unternehmung unterliegt (z. B. Datenschutzgesetz, Basel II oder Solvency II) oder welcher Nachweis von Sicherheitsstandards von Partnern gefordert wird. Für jedes Unternehmen ist es notwendig, einen Basisschutz sicherzustellen, auf dem man weitere technologische Massnahmen aufbauen kann. Viele Anforderungen einer Security Policy können heute elegant und einfach mit neuen Technologien gelöst werden. So kann z. B. das Reporting und Monitoring durch technische Lösungen erheblich erleichtert und Security messbar gemacht werden.



Pino Cuccaro, Senior Security Consultant

Um die Bereiche «Organisation» und «Mensch» umfassender zu betreuen, hat bw digitronik im Juni 2007 den ausgewiesenen Informationssicherheits-Fachmann Pino Cuccaro (36) als Senior Security Consultant verpflichtet. In den vergangenen Jahren hat er unterschiedlichste Positionen im Bereich IT Management und Informationssicherheitsberatung bekleidet. Er kennt die Herausforderungen auf der Unternehmensseite und kann sich darum als Security Consultant optimal in die Gedankenwelt seines Gegenübers einfühen. Vor seinem Engagement bei bw digitronik war er unter anderem als IT Security Projekt Manager für die Bank Sarasin und als Business Technologist für Security Management bei Computer Associates tätig. Um unsere Kunden besser unterstützen zu können, wird die Abteilung Security Consulting und Awareness in den nächsten Monaten um weitere Spezialisten ergänzt. Mit unserem ganzheitlichen Ansatz, der Organisation, Mensch und Technologie umfasst, können wir bestimmt auch Ihre Bedürfnisse abdecken. **Fordern Sie uns heraus!**