

Eine Studie des PONEMON Institutes unter Arbeitnehmern, die 2008 ihren Arbeitsplatz verloren oder gewechselt haben, zeigt: **59 Prozent** der Befragten haben beim Verlassen ihres vorherigen Arbeitgebers vertrauliche Unternehmensdaten, wie Kundenkontakte, mit sich genommen. Zudem hätten viele Fälle von Datenverlust durch bessere Datenschutzrichtlinien und entsprechende Technologien verhindert werden können.



**Arbeitnehmer gestehen Datenklau!**

53 Prozent der Befragten speicherten Informationen auf CD oder DVD, 42 Prozent auf einen USB-Stick und 38 Prozent verschickten Informationen per E-Mail-Anhang an eine private E-Mail-Adresse. **79 Prozent der Befragten nahmen Daten ohne Erlaubnis ihres Arbeitgebers mit.** 82 Prozent gaben an, dass ihr Arbeitgeber keine Durchsicht oder Prüfung elektronischer oder gedruckter Dokumente veranlasst hatte, bevor die Befragten ihren Arbeitsplatz verliessen. 24 Prozent hatten auch nach ihrem Weggang Zugriff auf das Computersystem oder Netzwerk ihres früheren Arbeitgebers.

**SCHUTZ IST MÖGLICH!**

Datenverluste können auch in Zeiten von Personalabbau verhindert werden. Es kann sicher gestellt werden, dass Angestellte sensible Informationen nicht an persönliche E-Mail-Adressen verschicken oder auf CD-ROM und/oder USB-Stick speichern.

Unternehmen sollten wirksame Technologien zum Schutz vor Datenverlust einsetzen, die vertrauliche Informationen schützen und Missbräuche verhindern. Das Überwachen der Daten sowie verschlüsseln von Netzen und Peripherie ist ein zentrales Thema.

**Informationsüberblick**

Die Idee <Verschlüsselung versus DLP>	2
Daten Verschlüsselung warum?	2
DIE LÖSUNG <b>Crypto One</b>	3
FUNKTIONSPRINZIP <b>Crypto One</b>	3
DAS UNTERNEHMEN CRYPTOSWISS AG	4
Wir sorgen für ihre Sicherheit	4

# Die Idee <Verschlüsselung versus DLP>

Der europäische IT-Security-Markt wächst in den nächsten Jahren zweistellig, erwarten die Analysten. Manchen Bereichen könnte allerdings der steigende Druck zum Kostensparen den Schwung nehmen, etwa der hochgepreisene Anti-Datenleck-Technik **Data Loss Prevention (DLP)**.

Der Schutz sensibler Daten steht für viele Unternehmen ganz oben auf der Agenda, allerdings ist der firmenweite Einsatz klassischer Verschlüsselungs-Tools die kostengünstigere Variante als die derzeitige „Hype-Technik“ **DLP**.

Auch die CRYPTOSWISS sieht in der Verschlüsselung einen der drei Kernbereiche, auf den sich Firmen derzeit in Sachen Security konzentrieren sollten. Das zeigten nicht zuletzt spektakuläre Fälle von Datenverlust. So hatten die britische Steuer- und Wohlfahrtsbehörde HM Revenue and Customs (HMRC) sowie zuletzt die Grossbank HSBC, unverschlüsselte CD mit Unmengen sensibler Informationen verloren. Mit **Crypto One** wäre das nicht passiert, respektive sind die Daten verschlüsselt und für Unberechtigte nicht lesbar!

## DATEN VERSCHLÜSSELUNG WARUM?

Elektronische Daten wie Verträge, Kundendaten, Studien, Pläne etc. sowie vertrauliche und wichtige Korrespondenz ist ein wertvolles und schützenswertes Kapital eines Unternehmens.

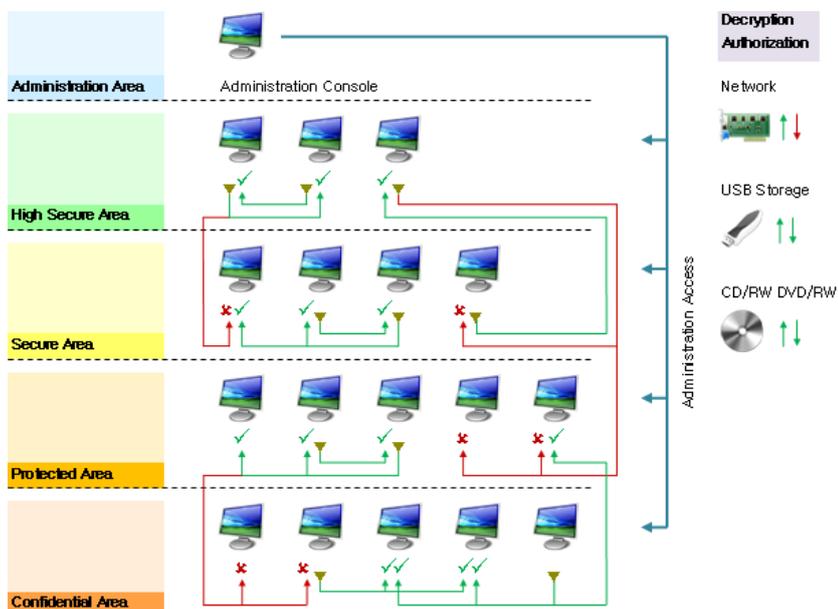
**Crypto One** ist ein Sicherheits- und Verschlüsselungssystem, welches alle Daten in einem geschlossenen und sicheren Umfeld unverschlüsselt zum bearbeiten belässt. Sobald diese Daten das sichere Umfeld verlassen, sei es über das Netzwerk oder externe Speichermedien (USB-Stick, CD-ROM etc.) werden die Daten verschlüsselt und können nur von einem anderen, legitimierten **Crypto One** Benutzer wieder gelesen und bearbeitet werden.

**Crypto One** bietet somit die absolute Sicherheit aller Daten, ohne das Verteilen und Aufbewahren von

Schlüsseln und das Administrieren von komplexen Berechtigungstabellen.

### Highlights von **Crypto One**

- ⇒ Echtzeit Verschlüsselung aller Daten über das Netzwerk (LAN, WAN etc.)
- ⇒ Verschlüsselter Datenaustausch über COM-Schnittstellen-Ports (Seriell, USB, etc.)
- ⇒ Sperrung oder Verschlüsselung von Daten ins Internet
- ⇒ Kontrollierter und koordinierter Datenaustausch über das Email mit wahlweiser Verschlüsselung der Daten oder das versenden von unverschlüsselten Informationen an definierte Empfänger.
- ⇒ Verschlüsselung aller portablen Speichermedien, wie externe Disk, USB-Stick, CD-ROM DVD etc.
- ⇒ Datenbearbeitung und -austausch zwischen Datenbanken und Benutzern, sind verschlüsselt.
- ⇒ Verschlüsselung des lokalen Dateisystems
- ⇒ Verschiedene Verschlüsselungsverfahren wählbar
- ⇒ Schlüssellängen variabel, 512 Bit...
- ⇒ Einsatz Neuronales Netz (Schlüsselberechnung)
- ⇒ Hierarchisches Sicherheitssystem
- ⇒ Keine Benutzerschulung notwendig



**CRYPTO ONE** ist eine Verschlüsselungssoftware, welche sensible Daten von Unternehmen vor dem Zugriff durch Unberechtigte schützt, ohne dabei den gewohnten Arbeitsablauf zu stören. Dies wird durch die Verschlüsselung von Daten erreicht, welche innerhalb eines Netzwerkes ausgetauscht werden. Somit können nur noch **CRYPTO ONE** User miteinander kommunizieren.

## Verschlüsselungsprinzip

Das Sicherheitssystem **CRYPTO ONE** basiert auf den neusten Erkenntnissen der Encryption-Technologie. **CRYPTO ONE** verschlüsselt Datenpakete bei deren Übermittlung in Echtzeit, ohne einen Schlüssel mitzuliefern. Es können wahlweise 6 verschiedene und bewährte Verschlüsselungsverfahren, wie DES, Triple-DES, RC2, Rijndael und AES verwendet

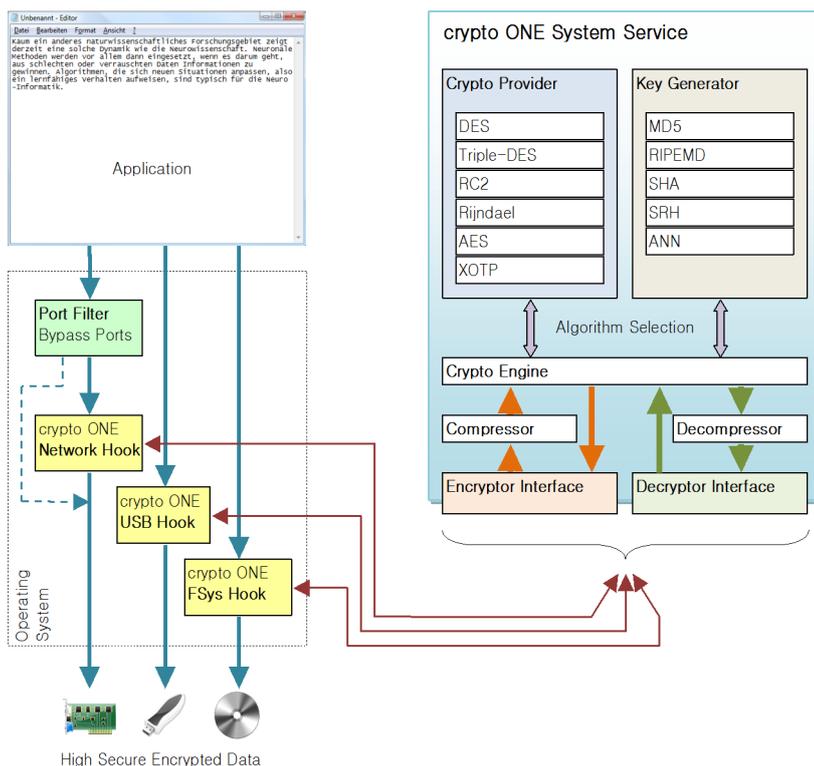
werden. Zusätzlich hat die CRYPTOSWISS ein Verschlüsselungsverfahren entwickelt (XOTP), welches auf der Philosophie des One-Time-Pad basiert.

Mit **CRYPTO ONE** wurde ein Verfahren entwickelt, welches das Übermitteln eines Schlüssels unnötig macht, da dieser zum Teil in Form eines dynamischen Algorithmus bereits in den zu übertragenden Daten enthalten ist und auch durch diese definiert wird. Zu diesem Zweck stehen bis zu 5 verschiedene Hash-Algorithmen für die automatische Schlüsselberechnung zur Verfügung. Bei **CRYPTO ONE** werden beim Versenden der Datenpakete keine kompletten Schlüssel mitgeliefert. Die verschlüsselten Datenpakete werden zusätzlich um 1/3 (kleiner) komprimiert.

## FUNKTIONSPRINZIP

Die Anwender der **Crypto One** Technologie verfügen innerhalb ihrer Datenumgebung über eine <codierte> Installation. Die in diesem Netzwerk installierten Geräte haben nur dann den Zugriff auf die Unternehmensdaten, wenn sie mit **Crypto One** ausgerüstet sind und somit Daten entschlüsseln wie auch verschlüsseln können.

Über einen Administrator kann **Crypto One** konfiguriert und überwacht werden. Jeder einzelne Arbeitsplatz und Server wird über das <Monitoring-Tool> in Echtzeit während 24h kontrolliert und allfällige Vorfälle, wie Daten auf ein Medium schreiben, werden aufgezeichnet und in einem <Logfile> gespeichert.



Es besteht die Möglichkeit, verschiedene Sicherheitsstufen zu konfigurieren, wie <vertraulich> bis <hochsicher> sowie ein hierarchisches Sicherheitssystem, welches nur Daten auf der selben oder höheren Stufe zulässt (Abteilungsleiter kann auf Daten der Mitarbeiter zugreifen aber nicht umgekehrt).

**Crypto One** kontrolliert sich selbst mit einer Systemintegritätsprüfung in Echtzeit und leitet automatische Sperrungen ein, sobald am Sicherheitssystem manipuliert wird.

**Crypto One** ist als Treiber zu installieren und kann nur vom **Crypto One** Administrator konfiguriert oder deinstalliert werden. Dazu wird eine Lizenznummer und ein Hardware Dongle benötigt.



## cryptoswiss AG

Freyastrasse 14  
P.O. Box

CH-8026 Zürich

Tel: +41 (0)44 787 30 00

Fax: +41 (0)44 787 30 05

Mail: [info@cryptoswiss.ch](mailto:info@cryptoswiss.ch)

Web: [www.cryptoswiss.ch](http://www.cryptoswiss.ch)

ANALYSE— RISK—  
SECURITY SOLUTIONS

[www.cryptoswiss.com](http://www.cryptoswiss.com)

*CRYPTOSWISS ist ein Unternehmen, das sich auf die Beratung, die Analyse und die Optimierung von Sicherheitssystemen sowie das Erstellen von Sicherheitsrichtlinien und Gefährdungsanalysen spezialisiert hat. Die Entwicklung und der Vertrieb von <Data Encryption Systems>, Daten- und Netzwerksecurity-Solutions sowie <Data Loss Preventions> (DLP) Systeme für Banken, Finanzinstitute, Industrie und KMU's erweitert die Kompetenz der CRYPTOSWISS.*

*Das Unternehmen mit Sitz in Wollerau unterhält Niederlassungen in Zürich sowie Vertriebspartner in der gesamten Schweiz und Europa.*

*CRYPTOSWISS Partner und Mitarbeiter verfügen über mehrere Jahre Erfahrung und eine hohe Kompetenz in den Bereichen IT, Informatik, Security und Datenverschlüsselung bei Projekten in der Industrie, Finanzwirtschaft und bei Banken.*

*Die internen und externen Spezialisten der Firma CRYPTOSWISS zeichnen sich aus durch ein enormes Fachwissen und ausgewiesene Erfolge in den Bereichen Beratung, Analysen, Netzwerksicherheit sowie Daten- und Softwaresicherheit. Projektleitung, Risikoanalysen und das erstellen von Sicherheitsrichtlinien und Gefährdungsanalysen. Fokussiert auf die grösstmögliche Sicherheit von vertraulichen Unternehmensdaten, ist die CRYPTOSWISS ein verlässlicher Partner in Sicherheitsfragen.*

## WIR SORGEN FÜR IHRE SICHERHEIT

Unsere qualifizierten Spezialisten unterstützen Sie bei der **Planung, Implementierung und Betreuung** der auf Ihre Bedürfnisse **zugeschnittenen Lösung**. Wir kennen die Produkte der führenden Hersteller und wählen jeweils das Passende auf Grund der vorher gemeinsam mit Ihnen festgelegten Kriterien aus.

Wir sind zudem bestens vertraut mit den gängigen Standards. Sei es mit **S/MIME** oder **OpenPGP** im Bereich der E-Mail-Verschlüsselung oder mit den verwendeten symmetrischen Algorithmen (3DES, AES, Rijndael, One-Time-Pad, Neuronale Netze) bei der Festplattenverschlüsselung. Natürlich implementieren wir für Sie auch weiter entwickelte Techniken wie tokenbasierte Authentisierung oder Single-Sign-On.

Wir beraten Sie fundiert und entscheiden mit Ihnen, ob nicht eventuell selbst ausgeteilte Schlüssel ausreichend sind.

Testen Sie uns und nehmen Sie mit uns Kontakt auf:

Telefon: +41 (44) 787 30 00

Email: [info@cryptoswiss.ch](mailto:info@cryptoswiss.ch)

