GEHEIMHALTUNG HAT ZAHLREICHE DIMENSIONEN

OFFICE SECURITY UND SECURE DIPLOMATIC MESSAGING

Staatliche Organisationen pflegen traditionell eine ausgeprägte Geheimhaltungskultur. Die globalen Informationsrisiken und der Technologiewandel zwingen sie jedoch dazu, ihre Security Policies stetig zu optimieren. Im täglichen Umgang mit höchst sensiblen Informationen ist deshalb eine Sicherheitslösung, die alle vorkommenden Arbeitsprozesse des «Büroalltags» einschliesst, unverzichtbar. Dafür bietet Crypto AG, Ihren Bedürfnissen angepasst, zwei Sicherheitslösungen an: Die Crypto Desktop HC-9300 Plattform mit individuell wählbaren Security Applications und das Secure Messaging System «CAG MAIL».

von Beat Püntener, Product Manager

Wie leicht und schnell geht es, eine grosse Menge an Informationen auf einen USB-Stick zu kopieren – und wie schwierig oder praktisch unmöglich ist es zu kontrollieren, was nachher mit diesen Informationen passiert. Insofern besteht heute ein enormer

Unterschied zu den Zeiten, als Dokumente und Archive noch vorwiegend auf Papier beruhten. Die riesigen Informations- und Datenmengen, welche heute erzeugt, verarbeitet, gespeichert und kommuniziert werden, lassen deshalb ein Projekt für Informationssicherheit leider oft zu einem Schreckensszenario mutieren. Lecks können zu einer veritablen Katastrophe führen, dies bedeutet jedoch nicht, dass Organisationen diesen Risiken einfach ausgeliefert sind. Was sie benötigen, ist in erster Linie eine durchdachte Security Policy. Diese dient als Grundlage zum Aufbau der nötigen Sicherheitsstrukturen und -prozesse.

Vertrauliche Informationen sind in jedem Zustand gefährdet

Eine vertrauliche Information ist bereits während ihrer Entstehung vertraulich und muss bei der Erfassung und späteren Bearbeitung entsprechend behandelt werden. Das heisst, dass vom ersten Moment an ihre Klassifizierung und damit auch die Zugriffsberechtigungen festgelegt sein müssen. Je nach Schutzgrad bedeutet das, dass Vorgänge wie Ausdrucken, Kopieren, Versenden oder Umklassierung verhindert werden müssen. Die Durchsetzung dieser Anforderungen wird durch organisatorische und technische Massnahmen sichergestellt. Diese werden in Form einer Security Policy festgehalten. Zu den technischen Massnahmen gehört im Wesentlichen der Einsatz von Chiffriergeräten, welche mit kryptografischen Verfahren und anderen Sicherheitsfunktionen die technisch möglichen Aspekte der Security Policy konsequent durchsetzen. Dabei gilt es die folgenden Bereiche zu beachten:

Bearbeitung von Information

Zugang zum Klartext für die Ausgabe oder weitere Bearbeitung darf ausschliesslich autorisierten Personen gewährt werden. Ist dieser Zugang vorhanden, gilt es die daraus folgenden Schwachstellen zu eliminieren. Einerseits besteht die Gefahr, dass die Information durch ungewollte Abstrahlung, sei es elektrisch, akustisch oder optisch für Aussenstehende sichtbar wird. Anderseits ist es zu verhindern, dass die Information aus der gesicherten Umgebung entfernt oder unerlaubt kopiert wird. Dies kann durch technische Massnahmen verhindert oder zumindest erschwert werden. Dazu gehören lückenlose Protokollierungen, woraus ersichtlich ist, wer wann was womit gemacht hat.

Übermittlung von Information

Während der Übermittlung von Informationen erfolgt der Transfer meist durch ungeschützte Bereiche (z.B. WAN), in denen alle denkbaren Attacken möglich sind. Nur durch eine Verschlüsselung auf höchstem Niveau kann das Informationsrisiko (Informationsleck) in dieser Zustandsphase (Übergangsphase, Übertragungsphase) zweifelsfrei ausgeschlossen werden. Eine zuverlässige Übermittlung der Informationen gehört im weiteren Sinne auch zum Thema Verfügbarkeit.

Krisenresistente Übertragungssysteme, die beim Ausfall von Kommunikationskanälen beispielsweise automatisch auf andere Medien ausweichen, sind hier einfachen Systemen weit überlegen.

Speicherung von Information

Ebenso risikobehaftet ist die Speicherung der Information – was immer wieder durch Meldungen über Hackerangriffe auf Rechner und Websites von Behörden bestätigt wird. Nebst der Vertraulichkeit der Informationen ist auch die Verfügbarkeit gefährdet. Wer dies total ausschliessen will, benötigt eine High-Security-Speicherlösung, welche sowohl die Vertraulichkeit sicherstellt als auch gleichzeitig den Verlust oder die Manipulation von Daten verhindert oder zumindest erkennt.

Ein dermassen durchgängiges Sicherheitskonzept bei den eingesetzten Sicherheitslösungen verhindert, dass Informationen in einen «Gefährdungszustand» geraten können. Darüber hinaus sind organisatorische Sicherheitsmassnahmen nötig, die wirksam werden, wenn Informationen im Rahmen der auftragsgemässen Organisationstätigkeit den internen Schutzbereich verlassen. Beispielsweise zur Unterstützung einer Verhandlungsführung.

Die Kernkriterien einer nachhaltigen Security Policy

Die Security Policy einer Organisation oder eines Unternehmens geht von einer umfassenden Sicherheitsanalyse aller Bereiche aus und mündet in der Formulierung von Vorschriften und Schutzmechanismen. Sie ist ihrem Charakter nach «defensiv» – im Sinne des «Need to know»-Prinzips. Dies bedeutet: Nur Personen, welche sensible Informationen für ihre Arbeit benötigen, sollten darauf Zugriff haben. Eine Security Policy muss jedoch noch viel weiter gehen. Sie sagt z. B. aus:

- welche Informationen sensibel sind
- wer darauf Zugriff hat
- wie man mit diesen umgeht
- wie sie gekennzeichnet und klassifiziert werden
- wo und wie sie abgelegt oder gespeichert werden (z. B. nur lokal)
- wie sie kommuniziert werden (Schutzmechanismen, Adressaten)

Die Security Policy enthält die Vorgaben für die praktische Implementation von technischen und operativen Sicherheitszonen – mit unterschiedlichen Sicherheitsansprüchen. Dies schliesst unter anderem Clearance (Rechte), Rollen und Pflichten der autorisierten Benutzer mit ein. Eine aufzubauende Sicherheitstechnologie muss diese Auflagen optimal umsetzen können.

Eine Security Policy kann nur eingehalten werden, wenn sie durch organisatorische Massnahmen und technische Sicherheitslösungen erfolgreich umgesetzt werden kann.

Sicherheitsarchitektur im Office ist Voraussetzung für Hochsicherheit

In einer modernen Arbeitsumgebung sind alle Applikationen und Technologien miteinander verknüpft. Deshalb kann nur eine lückenlose Sicherheitskette – die perfekt auf die verwendeten Technologien zugeschnitten ist – die gewünschte Sicherheit bieten. Genau aus diesem Grund umfasst Crypto's Security-Architektur nebst der Verschlüsselung auch die anderen Aspekte wie konsequenten Zugriffsschutz mit Klassifizierung und benutzerspezifischer «Clearance», Abstrahlsicherheit («COMPREM»), «Tamper Resistant Design» sowie die verschlüsselte Speicherung aller Informationen usw.

Officelösungen: Crypto Desktop HC-9300 für Officeapplikationen

Das Crypto Desktop HC-9300 und die dafür erhältlichen «Security Applications» wurden auf die High-Security-Bedürfnisse im stationären Office ausgelegt. Diese Lösung basiert auf unserer neuen Plattformidee: HC-9300. Ein modernes Desktop-Chiffriergerät, auf dem «Security Applications» wie Fax-, Voice- oder File Encryption implementiert sind und dem Anwender Sicherheit, Effizienz, Verfügbarkeit und Investitionsschutz garantieren.

Komplettsystem: Sicheres Messaging für die Diplomatie

Das Secure Diplomatic Messaging System «CAG MAIL» ist auf die speziellen Bedürfnisse einer diplomatischen Organisation zugeschnitten. Meldungsbearbeitung und Kommunikation zwischen exponierten Stellen wie Botschaften und dem Ministerium wird umfassend mit Fokus «höchste Sicherheit» konsequent gelöst. Dies bietet den Vorteil, dass die eingespielte Arbeitsweise einer diplomatischen Organisation beibehalten werden kann.

Abläufe und Arbeitsweise sind immer Organisationsspezifisch. Deshalb legen Sie in Zusammenarbeit mit unseren Experten fest, wie die konkrete Lösung aussehen soll.

Das sichere diplomatische Messaging-System besteht aus den Komponenten «Crypto Workstation» und dem «Crypto Message Server».

Zur abstrahlungssicheren Workstation gehören Drucker und Scanner inklusive Messaging-Applikation und Standard-Office-Tools. Workstation und Server sind via LAN und IP/VPN miteinander verbunden.

Über individuelle Mailboxen, Dokumentenklassifizierung, «Identity based User Access» mit «User Clearance» stehen genau die Schutzmechanismen zur Verfügung, die ein umfassendes Sicherheitssystem benötigt.

Eine einmal im System erfasste Meldung kann nicht mehr umklassiert werden. Damit wird eine wichtige Policybestimmung konsequent umgesetzt und verhindert, dass Dokumente deklassiert und publik gemacht werden können. Der Sender einer Nachricht ist dank Meldungs-Tracking jederzeit über den Status seiner Nachricht informiert. Er wird benachrichtigt, wenn der Empfänger die Nachricht erhalten und gelesen hat. Durch all diese Vorkehrungen erhalten die Meldungen eine Verbindlichkeit und damit einen offiziellen Charakter. Dadurch ist sichergestellt, dass auch nach Monaten der Informationsfluss noch lückenlos nachvollziehbar ist.

Der «Crypto Message Server» kann automatisiert über mehrere Medien kommunizieren und gewinnt dadurch das Vertrauen der Benutzer. Beim Ausfall eines Kommunikationskanals wie z. B. des IP-Netzes kann der Meldungsaustausch automatisch über Satelliten, Telefonleitung oder Funk geleitet werden. Nicht nur die Redundanz kann bei der Wahl des Kommunikationskanals eine Rolle spielen, sondern auch die Priorisierung. Eine Meldungspriorisierung stellt sicher, dass die wichtigen Meldungen entsprechend Ihrer Priorität behandelt werden. Die Übermittlungsstrategie kann für jede der drei Prioritäten individuell festgelegt werden. So entscheiden Sie über die Gewichtung zwischen Übertragungsdauer und Kosten.

Besonderheit

«CAG MAIL» ist ein komplett geschlossenes System. Es ist nicht möglich, Meldungen elektronisch aus dem System zu entfernen. Damit ist die Gefahr eines Datendiebstahls abgewendet. Der Betreiber profitiert von den Vorteilen der neuen Technologien ohne die sonst üblichen damit verbundenen Nachteile.

Fazit

Drei Faktoren sind für den Erfolg einer sicheren Messaging-Lösung verantwortlich.

1. Das System arbeitet nach individuellen kunden- und policyangepassten Arbeitsabläufen und nicht umgekehrt.
2. Die systematische Integrationsfähigkeit des sicheren Messaging-Systems in eine bestehende Kommunikations-Infrastruktur muss gewährleistet sein.
3. Ein einfaches Sicherheitsmanagement verhindert Fehler im täglichen Betrieb.