ner ou de mettre en place un logiciel d'encryptage des fichiers.

Et n'oubliez pas notre Assemblée générale le 14 mars 2001 à Berne! Nous aurons l'occasion de renforcer la présence romande au comité en y accueillant un nouveau membre et Peter Bitterli nous présentera un cas pratique de piratage bancaire…

Michel Huissoud, vice-président

Encryption

Anforderungen an eine File-/Folder-Verschlüsselungssoftware

Vor noch nicht allzu langer Zeit wurde das firmeninterne Netz als sicher angesehen. Informationen wurden entweder auf lokalen Workgroup-Servern oder aber Abteilungsservern abgelegt. Mitarbeiter arbeiteten nur an ihren lokalen PCs, Informationen gelangten kaum ausserhalb der Firma. Diese wurden, wenn überhaupt, maximal mit einem Passwort geschützt. Mittlerweile hat sich dieses Umfeld jedoch stark geändert. Informationen werden auf grossen Unternehmensservern gespeichert, die Grenzen des firmeneigenen Netzwerkes sind durch Firmenübernahmen und Kooperationen nicht mehr so genau definiert, Mitarbeiter arbeiten oft mit Laptops, d.h. die Informationen gelangen immer mehr ausserhalb des physischen Sicherheitsbereiches der Firma. In diesem Zusammenhang wird auch die Frage nach einem besseren Schutz der Informationen sowohl gegen Diebstähle von Aussen, als auch gegen Zugriff von Innen (z.B. bei Salärangaben oder kundenspezifischen Daten) immer aktueller. Eine mögliche Form ist dabei die sogenannte File-/Folderverschlüsselung, bei der Dateien (Files) und Ordner (Folder) verschlüsselt abgelegt werden. Dieser Artikel soll einen Überblick über die verschiedenen Aspekte bei der Evaluation und Einführung einer solchen Software geben.

Verschlüsselung – eine kurze Einführung

Grundsätzlich unterscheidet man die Verschlüsselung mit sogenannten symmetrischen Schlüsseln (secret key) und asymmetrischen Schlüsseln (public key). Der Unterschied besteht darin, dass beim symmetrischen Verfahren der gleiche Schlüssel zur Ver- und Entschlüsselung benutzt wird, während beim asymmetrischen Schlüssel je ein unterschiedlicher Schlüssel eingesetzt wird. Der Nachteil bei den symmetrischen Verfahren liegt darin, dass beim Austausch einer Meldung beide Parteien über den gleichen Schlüssel verfügen müssen. Der Vorteil liegt in der geringeren Schlüsselgrösse (128-bit wird als sicher angesehen) und in einer schnelleren Verschlüsselung. Asymmetrische Verschlüsselungsverfahren haben den Vorteil, dass zwei Parteien die Schlüssel nicht zuerst austauschen müssen. Der Nachteil liegt darin, dass die Verschlüsselung der Files langsamer erfolgt und der verschlüsselte Text grösser ist als bei der symmetrischen Verschlüsselung. Im Zusammenhang mit der File-/Folder-Verschlüsselung werden vor allem symmetrische Verfahren eingesetzt. Gängig sind in diesem Zusammenhang Triple-DES oder IDEA.

File-/Folder Verschlüsselung

Die Komplexität der Handhabung von File-/Folder-Verschlüsselungslösun-

gen ist jedoch je nach Anwendungsbereich und Anzahl Benutzer sehr unterschiedlich. Die Komplexität bezieht sich dabei nicht nur auf die Technologie an sich, sondern vor allem auch auf deren Handhabbarkeit in einem firmenweiten Umfeld mit einer grossen Anzahl Benutzer. Als "Sicher" im Sinne der unterstützten Verschlüsselungsalgorithmen können wohl alle im Markt verankerten Verschlüsselungsprodukte angesehen werden.

Im Falle eines privaten Benutzers, der seine Informationen schützen möchte, lässt sich das Problem einfach lösen. Der Benutzer schützt seine Daten mit einer Verschlüsselungssoftware; kein anderer Benutzer muss das Passwort kennen, kein anderer zwingend auf die Daten zugreifen. Er selbst verwaltet seinen Schlüssel, welcher nur lokal auf seinem PC liegt. Die Anforderungen an die Software bezüglich Einfachheit der Administration von Benutzern und Benutzergruppen sind minimal. Er entscheidet zudem selbst, welche Files und Folders verschlüsselt werden sollen und welche nicht.

Zentrale Administration

Im Falle von grösseren Installationen gestaltet sich jedoch die Angelegenheit zunehmend schwieriger. Augenfälligstes Problem ist die Zunahme der Benutzer und damit verbunden das Bedürfnis nach Administration von einem zentralen Punkt aus. Können zum Beispiel bei einer Schlüsselerneuerung (Key Rollover) bei einigen wenigen Benutzern diese noch mittels Disketten vom Supportpersonal selbst ausgeführt werden, ist dies bei einigen 100 oder gar 1000 Benutzern nicht mehr möglich. Hier kann es eine Anforderung sein, dass das Produkt eine Script-Sprache beinhaltet, mittels derer die Schlüssel an die User verteilt werden können. Im weiteren ist es wichtig, die Integration mit anderen Systemadministrationsprodukten wie z.B. Tivoli, Microsoft SMS oder CA TNG zu prüfen. Auch hier können allenfalls Synergien gewonnen werden. Als Spezialfall eines Key Rollovers kann der sogenannte Key Compromise erachtet werden. Nimmt ein User an, dass sein Passwort bekannt wurde oder eine 3. Person unberechtigt Zugriff zu seinem Schlüssel erhielt, d.h. sein Schlüssel sehr wahrscheinlich kompromittiert wurde (key compromise), muss die Administration den Schlüssel als ungültig erklären und durch einen neuen ersetzen können. Generell ist bei solchen Schlüsselerneuerung darauf zu achten, dass diese möglichst transparent, d.h. für den Benutzer und den Administrator einfach, zu handhaben sind.

Falls die Benutzer intern oft wechselnde Arbeitsplätze haben (Roaming Users) oder aber via Remote Zugriff auf das Firmennetz zugreifen (Mobile Users), entstehen weitere Anforderungen. Die Schlüsselinformationen müssen im Fall der Roaming Users zentral, d.h. vom lokalen PC unabhängig, zugänglich gemacht werden. Im Fall der Mobile Users ist genau das Gegenteil der Fall. Die Schlüsselinformationen müssen lokal, d.h. netzwerkunabhängig zur Verfügung stehen. Diese zwei Anforderungen können unter Umständen im Widerspruch zueinander stehen und sind auch von der internen Sicherheitspolitik abhängig.

Gruppenbildung

Im Zusammenhang mit der Benutzerverwaltung steht das Problem der Gruppenbildung, d.h. dass mehrere Personen oder Gruppen geschützt auf ein File resp. Folder Zugriff haben müssen. Hier ist es vor allem wichtig, dass Benutzer dynamisch Gruppen zugeordnet und wieder aus ihnen entfernt werden können. Diese Funktionalität ist längst nicht selbstverständlich. Je nach Lösungsansatz werden bei einzelnen Produkten bei Gruppenverschlüsselung nämlich die Files mit jedem Schlüssel der Gruppenmitglieder verschlüsselt. Tritt nun ein Mitarbeiter aus der Gruppe aus oder wird neu ein Mitglied dieser Gruppe, muss dieser Vorgang für jedes File mit den neuen Gruppenmitgliedern vorgenommen werden. Lösungen dieser Art machen es sehr schwierig, dynamisch Gruppen zu bilden oder Benutzer dieser Gruppen zuzufügen respektive zu entfernen. Als eine spezielle Art der Gruppenbildung kann die Delegationsfunktion angesehen werden. Geht ein Mitarbeiter in die Ferien, so sollen ein oder mehrere Stellvertreter Einsicht in die verschlüsselten Dateien haben können. Abgeklärt werden muss in einem solchen Fall, ob diese bereits zum Zeitpunkt der Verschlüsselung bekannt sein müssen oder aber später definiert werden können, ohne dass das File ent- und wieder verschlüsselt werden muss.

Integration mit anderen Sicherheitsprodukten

In grösseren Firmen ist oftmals bereits eine Sicherheitsinfrastruktur im Einsatz, sei dies ein Single-Sign-On-Produkt oder bereits eine Public Key

Infrastruktur (PKI). Hier ist wichtig, dass sich das File/Folder-Verschlüsselungsprodukt in die bestehende Software integrieren lässt. In gewissen Bereichen kann die Integration der Produkte sogar noch weiter gehen: PKI-Produkte weisen üblicherweise sehr grosse Funktionalität im Bereich des User-Managements und der automatisierten Schlüsselverteilung auf. Hier können sogar wesentliche Synergien genutzt werden.

Was und wo wird verschlüsselt

Generell gesehen macht es keinen Sinn, alle Informationen zu verschlüsseln, da eine Chiffrierung immer auch mit gewissen Nachteilen behaftet ist. So kann es sein, dass die Filegrösse durch die Verschlüsselungsinformationen markant vergrössert wird, d.h. mehr Speicherplatz für die Dateien zur Verfügung gestellt werden muss. Ebenfalls bemerkbar für den User macht sich die Wartezeit, während der das System die Datei ent- resp. verschlüsselt sowie die vermehrte Eingabe von Passwörtern.

Bei gewissen Produkten lässt sich einstellen, ob auch Programmfiles wie z.B. exe- oder sys-Dateien verschlüsselt werden sollen. Werden diese unverschlüsselt belassen, hat dies den Vorteil, dass der PC oder der Laptop sich auch bei vergessenen Passwörtern noch starten lässt. Einzig der Zugriff auf die geschützten Dateien wird verwehrt. Als potentielle "Sicherheitslöcher" gelten die Swap-Files und die temporären Dateien (*.tmp), die von den einzelnen Anwendungen angelegt werden. Deshalb ist bei einer Evaluation zu prüfen, ob diese temporären Dateien ebenfalls die Information verschlüsselt enthalten oder aber als versteckte Überreste auf dem System liegen bleiben.

Werden die Dokumente serverseitig abgelegt, ist zudem zu beachten, dass die Files oftmals auf dem Server entschlüsselt und auch auf diese Weise über das Netzwerk transportiert werden, d.h. die eigentliche Übermittlung erfolgt unverschlüsselt (z.B. beim Encrypted File System von Windows 2000). Dies kann verhindert werden, indem die Dokumente verschlüsselt übermittelt und erst auf dem Client entschlüsselt werden. Diese Funktionalität muss jedoch speziell vom Produkt unterstützt werden.

Betriebsproblematik

Die Erfahrung zeigt, dass vor allem auch der Betrieb einer solchen Infrastruktur bei grösseren Firmen sehr viel Aufwand bedeutet. Nebst der normalen Administrationsarbeit (Userverwaltung, Folderverwaltung), sind vor allem auch die täglichen Supportaufgaben nicht zu unterschätzen. Nimmt man an, dass jeder User ca. 2–3 Mal pro Jahr sein Passwort vergisst, kann dies bei grösseren Firmen schon zu einem beträchtlichen Mehraufwand führen. Um dies zu erleichtern, kann es sinnvoll sein, ein unternehmensweites Master-Passwort zu definieren, mittels dem ein Administrator auf die Daten zugreifen resp. Soforthilfe leisten kann. In diesem Zusammenhang steht auch die Sicherung der Schlüssel, d.h. es muss gewährleistet werden, dass auch beim Austritt eines Mitarbeiters auf die verschlüsselten Dateien zugegriffen werden kann.

Eine weitere Problematik ergibt sich bei Betriebssystem-Updates oder Service-Pack-Installationen. Da die Verschlüsselungssoftware oftmals Einträge in die Registry macht oder System-DLL's ersetzt, muss genau getestet werden, was vom Update überschrieben wird und ob die Verschlüsselungssoftware anschliessend noch problemlos läuft.

Zusammenfassung

Als eine Art Checkliste kann folgende Liste der zu beachtenden Punkte angesehen werden:

- Bei wie vielen Benutzern soll die Software installiert werden? Welche Hilfe bietet mir die Software dazu?
- Wird die Definition von dynamischen Gruppen unterstützt? Wird eine Delegationsfunktion unterstützt?
- Welche Möglichkeiten bestehen zur selektiven Verschlüsselung? Sollen alle Files verschlüsselt werden oder nur eigene Office-Dateien? Wie werden SWAP- oder Temp-Dateien verschlüsselt?
- Wie wird ein Key-Rollover unterstützt?
- Wie wird der Administrator bei der Bewältigung der täglichen Arbeit unterstützt?
- Ist bereits ein Backup-Produkt integriert? Werden die Files verschlüsselt gesichert?
- Was passiert bei Updates der Betriebssystemsoftware?
- Habe ich bereits andere Sicherheitssoftware im Einsatz oder plane ich deren Einsatz? Kann das Produkt integriert werden oder erhalte ich sogar noch zusätzliche Funktionalität?
- Wo werden die Dateien verschlüsselt: auf dem Server oder auf dem

Client? Werden die Dateien ver- oder entschlüsselt gespeichert?

Generell ist zu sagen, dass Sicherheitssoftware nie vollständig transparent für den User ist. Sei dies über Fehlermeldungen beim Zugriff auf gesicherte Dateien, mögliche Verzögerung beim Öffnen oder Schliessen der Datei oder aber bei der zusätzlichen Dateigrösse. Bei der Evaluation einer File-/Folder-Verschlüsselungssoftware lohnt es sich deshalb, sich vorgängig über die eigenen Anforderungen klar zu werden, diese zu priorisieren und die Evaluation entsprechend seriös durchzuführen.

Monika Josi, Senior Consultant, PricewaterhouseCoopers, Zürich

Résumé: Exigences à l'égard d'un logiciel d'encryptage des fichiers

Les mécanismes de chiffrage à l'aide de clés symétriques ou asymétriques ne sont pas utilisés que dans le domaine des communications mais également pour protéger des fichiers de données sur un serveur. De tels programmes ont généralement recours à des clés symétriques, triple-DES ou IDEA par exemple.

La complexité de la mise en œuvre et les coûts d'exploitation d'un tel logiciel croissent avec le nombre d'utilisateurs. Bien que le renouvellement ou le remplacement des clés de chiffrement puisse se faire par échange de disquette, les logiciels appelés à être employés par plus d'une centaine d'utilisateurs devraient offrir des fonctionnalités permettant de procéder à cette opération via le réseau.

La formation et la gestion des groupes de collaborateurs ayant accès à des fichiers communs constituent des défis importants: il s'agit de gérer élégamment l'adjonction ou le départ d'une personne, ainsi que les cas d'accès en cas de remplacement.

Une attention particulière doit être accordée à l'intégration de ce logiciel dans l'infrastructure existante, que ce soit les systèmes d'exploitation ou les autres logiciels de protection comme par exemple l'infrastructure de gestion des clés publiques (PKI). Un tel programme pourra par exemple aider à résoudre les problèmes d'échange ou de renouvellement des clés symétriques.

Lors de la mise en place d'un système d'encryptage des fichiers il est important de définir de manière restrictive les fichiers à protéger. Une telle procédure est gourmande en espace-disque et en temps de réponse. La sélection des objets à protéger devra également tenir compte des particularités des systèmes d'exploitation et du mode de travail entre les clients et le serveur.

Encryption

Kryptografische Schlüssel

In den vergangenen Jahren wurde in den Nachrichten vielfach über angeblich spektakuläre Einbrüche in Verschlüsselungssysteme wie DES und 512-Bit-RSA berichtet. Oftmals wurde die Anfälligkeit der jeweiligen Verschlüsselungssysteme zu Recht mit den zu kurzen kryptografischen Schlüsseln erklärt. Zu oft aber wurden falsche Schlüsse gezogen, die in Aussagen wie "Verschlüsselungssysteme mit einer Schlüssellänge von weniger als 1024 bits sind unsicher" gipfelten. Dies ist natürlich alles andere als zutreffend.

Wenn es um die Länge von kryptografischen Schlüsseln geht, kommt es entscheidend darauf an, dass die Art des jeweiligen Verschlüsselungssystems eindeutig angegeben wird. Die Sicherheit traditioneller (symmetrischer) Verschlüsselungssysteme beruht auf Prinzipien und Mechanismen, die völlig anders sind als diejenigen, die in (asymmetrischen) Verschlüsselungssystemen mit öffentlichem Schlüssel verwendet werden.

Verschlüsselungssysteme mit öffentlichem Schlüssel (public key) basieren auf komplexen mathematischen Aufgaben wie der Faktorisierung von grossen Zahlen oder der Berechnung von Logarithmen in endlichen Körpern. Angriffe auf Systeme mit öffentlichem Schlüssel setzen die Lösung der zugrunde liegenden mathematischen Aufgabe voraus, deren Schwierigkeit durch die Länge des öffentlichen Schlüssels bestimmt wird. So müssen zum Knacken eines öffentlichen Schlüssels des RSA-Verschlüsselungssystems (benannt nach seinen

Erfindern Rivest, Shamir und Adleman) zwei grosse Primzahlen gefunden werden, deren Produkt dem öffentlichen Schlüssel entspricht. Die Methoden zum Auffinden dieser Primzahlen, die so genannten Faktorisierungs-Algorithmen, wurden in den 20 Jahren seit der Erfindung des RSA-Systems erheblich verbessert, und so wurde das zuvor als sicher geltende RSA-System mit 512-bit-Schlüsseln schliesslich 1999 als unsicher befunden, als eine Gruppe von Forschern einen solchen Schlüssel binnen weniger Monate knackte. Durch den Einsatz der heute verfügbaren modernsten Methoden und Technologien ist es gegebenenfalls möglich, RSA-Schlüssel mit bis zu 600–700 bits zu knacken, wobei Schlüssel mit über 800–900 bits jedoch als sicher gelten. Die meisten der heutigen Systeme mit Public Key, einschliesslich der auf einem geheimen Logarithmus basierenden Systeme, haben Schlüssel mit einer Länge von 1024 bits.

Bei einem gut gestalteten symmetrischen Verschlüsselungssystem besteht der einzig durchführbare Angriff darin, eine verschlüsselte Nachricht mit verschiedenen Schlüsseln so lange zu entschlüsseln, bis sich ein "vernünftiges" Ergebnis ergibt. Ein solcher Angriff wird als exhaustive key search (abschliessende Schlüsselsuche) bezeichnet. Da die Schlüssel symmetrischer Systeme über keine besonderen mathematischen Eigenschaften verfügen, muss ein Angreifer durchschnittlich die Hälfte aller möglichen Schlüssel ausprobieren, bis die richtige Lösung gefunden wird. Die Schlüssellänge bestimmt die Zahl der möglichen Schlüssel – es gibt 2^n mögliche Schlüssel der Länge n bit – und damit auch die Durchführbarkeit eines Angriffs mittels abschliessender Schlüsselsuche. Durch die Erhöhung der Schlüssellänge um ein einziges bit verdoppelt sich die Zahl der möglichen Schlüssel und somit auch die Rechenleistung (respektive die Zeit) für eine abschliessende Schlüsselsuche.

1998 wurde der Data Encryption Standard DES, ein symmetrischer Blockchiffrieralgorithmus mit 56-bit-Schlüsseln, durch abschliessende Schlüsselsuche erfolgreich geknackt. Mit einem speziellen, 200 000 Dollar teuren Computer und 1536 nur für diesen Zweck gebauten Mikrochips wurde die Aufgabe nach rund 3 Tagen ausgeführt. Unter der Annahme, dass dieser besondere Computer eine Leistung von mindestens 250 W erfordert, verbrauchte die gesamte zum Knacken eines einzigen DES-Schlüssels erforderliche Berechnung rund 18 kWh Energie. Wenn die gleiche Art von Technologie zum Angriff auf ein DES-ähnliches Verschlüsselungssystem mit 85-bit-Schlüsseln eingesetzt werden würde, wären insgesamt rund 9600 GWh erforderlich, um einen einzigen Schlüssel zu knacken. Dies entspricht in etwa der Energie, die ein Atomkraftwerk während eines Jahres erzeugt. Dabei werden die Zeit, die Kosten und die Energie zum Bau eines Systems, das einen solchen Angriff binnen angemessener Zeit ausführen könnte, noch nicht einmal berücksichtigt.

Kryptografische Schlüssel: Wie lang ist lang genug?

Schlüssel-länge	Schlüssel-möglichkeiten	Tests s/Computer	Anzahl Computer	Gebrauchte Zeit
40 Bit	1.1×10^{12}	10^9	10^3	1.1s
56 Bit	7.2×10^{16}	10^9	10^3	20h
80 Bit	1.2×10^{24}	10^9	10^3	38 000 Jahre
128 Bit	3.4×10^{38}	10^9	10^3	1.1×10^{19} Jahre
128 Bit	3.4×10^{38}	10^9	7×10^9	1.5×10^{12} Jahre

Entdeckungsrisiko

Diese und ähnliche Schätzungen, welche zudem potenzielle technologische Weiterentwicklungen in der Zukunft einbeziehen, zeigen, dass symmetrische Systeme mit Schlüsseln mit einer Länge von über 90 bits sicher sind und sicher bleiben werden. Die meisten der heutigen Systeme verwenden 128-bit-Schlüssel. Dies bedeutet, dass eine abschliessende Schlüsselsuche im genannten Beispiel mehr Energie erfordern würde, als in den nächsten hundert Millionen Jahren produziert wird. Auch der neue Advanced Encryption Standard (AES), welcher der Nachfolger des DES sein wird, verfügt über 128-bit-Schlüssel. Die zusätzlichen Modi des AES, die Schlüssel mit einer Länge von 192 und 256 bits verwenden, sind im Hinblick auf die Sicherheit nicht erforderlich.

Dr. M. Stadler, Crypto AG, Zug

Nachdruck mit freundlicher Genehmigung des Autors und der Crypto AG, Zug.

Résumé: Clés de chiffrement: qui croire?

On lit régulièrement que telle ou telle clé de chiffrement a été déchiffrée et n'est donc pas sûre. Qu'en est-il en réalité?

Les systèmes de chiffrement à clés asymétriques (clés publiques) ont recours à un algorithme qui ne permet pas facilement de remonter du résultat aux données de base. Avec du temps et des ressources, de tels algorithmes peuvent cependant être décortiqués, raison pour laquelle leur degré de sécurité est directement lié à la longueur de la clé. On admet aujourd'hui que la taille des clés offertes sur le marché (1024 bits) offre une excellente sécurité.

Les systèmes de chiffrement à clés symétriques (clés privées) ne peuvent être violés qu'en essayant de manipuler le message intercepté avec plusieurs clés jusqu'à que le test permette d'obtenir un résultat plausible. Là également la longueur de la clé est déterminante: chaque bit supplémentaire double le nombre de solutions possibles qui devraient théoriquement être testées. Il est admis que toutes les clés d'une longueur supérieure à 90 bits sont sûres. La plupart des logiciels offrent aujourd'hui des clés d'une longueur de 128 bits.

Encryption

Lucifer's time has run out

According to several news items, the American National Institute of Standards (NIST) chose a new standard for encryption. IBM's Lucifer, better known as DES (Data Encryption Standard) which had been heralded as THE standard by NIST for quite some time began to show its age and gradually lost its hallowed security myth. NIST recommended already years ago to use DES in triplicate only in order to maintain top security. It was the galloping development of technology and above all the increased speed of computers that made it relatively easy to break the encryption code. Hackers were catching up and needed to be put at bay.

NIST looked for an improved method and launched a contest. The winner was a Belgian team (Daemen/Rijmen) that submitted an algorithm entry under the name of "Rijndael". This product was chosen by NIST as the new AES (Advanced Encryption Standard).

The consequences for the IT auditor are obvious. She/he will have to review periodically the encryption standard in place (firm, client). She/he will have to evaluate the age of the standard chosen and question whether the method is still valid. It is very well possible that the table shown (see article of Dr. Markus Stadler, risk of detection) will have to revised drastically in the near or far future. The development of computer technology has taught us lessons in this direction since the invention of the Hollerith punch card quite a few times already…