auf der CeBIT Hannover 04.–09. März 2008

Herausforderungen und Ansätze für ein IT-Frühwarnsystem

Von

Dr. Günther Welsch
Geschäftsführer
TeleTrusT Deutschland e.V.

Ralf Dörrie
Experte für IT-Frühwarn- und CERT-Fragen

Seit geraumer Zeit schon werden IT-Frühwarnsysteme als präventive Ergänzung zu bereits bestehenden CERT-Strukturen für das übergreifende IT-Sicherheitsmanagement im nationalen Kontext diskutiert. Hierbei lässt man sich insbesondere von der Idee leiten, dass durch geschickte Analysetechnik von Anomalien im Internet, in lokalen Netzen und bei IT-Applikationen mit späterer Aggregation deutlich bessere Hinweise auf neue konkrete Bedrohungen und Gefährdungen ermittelt werden können als es heute durch bestehende CERT-Strukturen möglich ist. Bei einer erfolgreichen Realisierung eines IT-Frühwarnsystems würde insgesamt eine längere Vorwarnzeit vor neuen Gefährdungen zur Verfügung stehen, die dann genutzt werden könnte, um effektive Maßnahmen zur Milderung und Vermeidung von IT-Angriffen zu ergreifen. Möglicherweise könnte auch die Gefahr eines „Zero-Day-Exploits“ unter Umständen deutlich reduziert werden.

Bevor allerdings ein Frühwarnsystem tatsächlich einen effektiven Beitrag zum Sicherheitsmanagement leisten kann, sind noch wesentliche Elemente zu entwickeln. Heute stehen den Unternehmen dazu nur eine geringe Auswahl an sinnvollen Methoden zur Analyse und Bewertung sowie begrenzte technische und personelle Analysekapazitäten zur Verfügung. Es fehlen weitgehend eine interdisziplinäre Zusammenarbeit, Informationspolitiken und rechtliche Klärungen hinsichtlich Verwertbarkeit von Daten und Informationen.

Ziel eines IT-Frühwarnsystems

Das Ziel eines IT-Frühwarnsystems sollte es sein, die Sicherheit der genutzten ITK-Systeme nachhaltig zu erhöhen und die Infrastruktur widerstandsfähiger zu gestalten. Das Ziel soll erreicht werden, indem

- genauere Informationen bereitgestellt werden, um die Erstellung bzw. Verbesserung des tatsächlichen Lagebildes zu ermöglichen,
- Informationen zur weiteren Entwicklung von abstrakten Gefährdungen erarbeitet werden,
- konkrete Gefährdungen so frühzeitig erkannt werden, dass zielgruppengenau davor gewarnt werden kann, damit die Betroffenen geeignete Gegenmaßnahmen initiieren können.

Aufgaben eines IT-Frühwarnsystems

Ein IT-Frühwarnsystem soll mehrere Aufgaben wahrnehmen:

1. Konsolidierung eines übergeordneten und stimmigen IT-Sicherheitslagebilds unter Einbeziehung von aggregierten Daten und Informationen aus verschiedenartigen Quellen
2. Entwicklung von Trendanalysen bezüglich neuer abstrakter und konkreter Gefährdungen
3. Rechtzeitige Erkennung von konkreten Gefährdungen bzw. Gefahren durch Analyse und Bewertung geeigneter Daten und Informationen sowie die Warnung potenziell Betroffener

Der erste Punkt lässt sich mit einem definierbaren Aufwand erreichen. Die Güte des Lagebilds verhält sich mutmaßlich proportional zu den investierten Ressourcen. Unterschiedliche Ansätze eines Lagebilds existieren bereits. So betreibt das BSI ein Lagezentrum und bereitet eine IT-Lage auf. Im Internet gibt es zahlreiche Quellen, die unterschiedliche sicherheitsrelevante Informationen als Lagebilder anbieten. Diese Lagebilder sind jedoch meist nur rein technischer Natur. So werden beispielsweise die Häufung von Portscans oder Netzauslastungen dargestellt.

Ein stimmiges und übergeordnetes Lagebild, welches unter Einbezug von technischen Daten und Informationen aus sozialen Kontexten die Lage für interessierte Zielgruppen darstellt, gibt es noch nicht. Insbesondere sind in ein solches Lagebild Informationen und Erkenntnisse aus und zu verschiedenen Akteur- und Tätergruppen aufzunehmen, die für schädigende und/oder schadhafte Aktivitäten in Betracht gezogen werden müssen (Cracker, organisierte Kriminalität, feindliche/gegnerische Nachrichtendienste, etc.).

Der zweite Punkt setzt auf dem ersten Punkt auf. Ohne ein konsolidiertes Lagebild lassen sich keine Trends ableiten. Um werthaltige Informationen aufbereiten zu können, bedarf es engster Zusammenarbeit von Forschung, Wissenschaft, Herstellern, vertrauenswürdigen „Hacker-Communities“ und Sicherheitsbehörden.

Das rechtzeitige Erkennen von konkreten Gefährdungen und Gefahren ist die anspruchvollste und komplexeste Aufgabe. Um sie zu bewältigen, sind noch deutliche Anstrengungen zu unternehmen.

Die Herausforderung durch das Internet

Das Internet mit seiner Möglichkeit, global jedes angeschlossene System in Millisekunden erreichen zu können, bietet nicht nur den Platz für die sinnvolle Ausgestaltung von Wirtschaftsmodellen, sondern gleichzeitig auch Raum für kriminelle und schädigende Aktivitäten. Dabei sind die potenziellen Opfer stets in einer nachteiligen Situation, da sie meist nur lokal und fest an einen Ort gebunden sind, während Angreifer die gesamte Globalität und Anonymität des Internets für ihre Aktivitäten nutzen können. Eine solche Situation wird auch asymmetrische Bedrohungslage genannt.

Vor was soll rechtzeitig gewarnt werden?

Ein Teilziel eines IT-Frühwarnsystems ist die rechtzeitige Warnung vor neuen konkreten Gefährdungen, aber auch vor sich neu ergebenen abstrakten Bedrohungen (Trends). Welche Gefährdungen lassen sich dabei betrachten? Ausgangspunkt für die meisten Bedrohungen sind Schadprogramme bzw. Schadsoftware, welche

1. die Gutgläubigkeit des Anwenders ausnutzen,
2. neu bekannt gewordene Schwachstellen in einem IT-System oder einer Anwendung ausnutzen[1],
3. noch unbekannte Schwachstellen in einem IT-System oder einer Anwendung ausnutzen[2],
4. falsch administrierte IT-Systeme ausnutzen,
5. oder einen Designfehler in einer Standard-Funktionalität ausnutzen.

Weiterhin sind zu betrachten:

1. Massive Angriffe auf eine/mehrere IT-Plattformen mit dem Ziel der Verhinderung der Verfügbarkeit.
2. Gegen welche Systeme wird ein Schadprogramm eingesetzt und gegen wen (Wirtschaftsbranchen)?
3. Handelt es sich um einen Einzelfall oder reproduziert sich das Schadprogramm und breitet sich selbstständig aus?

Bei der zunehmenden Industrialisierung der Schadsoftware muss man davon ausgehen, dass neu gefundene Schwachstellen und Verwundbarkeiten in IT-Systemen kaum für flächenhafte, ungerichtete Angriffe ausgenutzt werden, sondern vielmehr für gezielte Angriffe auf wohldefinierte Opfer. Mit solchen speziell entwickelten Angriffswerkzeugen wird sich mehr Geld verdienen lassen als im Bereich der Massenangriffe, für die es keinen potenten Käufer gibt. Erst wenn die Schwachstelle größere Bekanntheit erlangt – sich also abgenutzt hat –, bietet sich das Recycling für Phising, Pharming und Co. an. Dies macht aber die besondere Herausforderung für ein IT-Frühwarnsystem deutlich, denn gezielte Angriffe auf einige wenige Opfer werden im großen Datenhaufen des Internets kaum zu verwertbaren Spuren führen.

Heutige Ansätze

Zum einen werden heute schon „IT-Frühwarnsysteme“ aus kommerzieller Hand angeboten, die über große Datenmengen und viele Sensoren verfügen. Wie die Auswertung erfolgt (rein technisch oder u.a. unter Einbezug von sozialen Kontexten) und welche weiteren Quellen hinzugezogen werden, bleibt häufig im Verborgenen. Ebenso ist unklar, inwieweit diese Art von Dienstleistungsangebot wirklich effektiv ist. Als freie Quelle ist z. B. das Internet Storm Center (s. a. S. 50) zu nennen, das ebenfalls

[1] *Die Schwachstelle oder Verwundbarkeit wird sichtbar durch das Re-Engineering eines Updates/Patches eines Herstellers.*
[2] *Der Zero-Day-Exploit*
[3] *http://internet-sicherheit.de/internet-analyse.html*
[4] *www.cert-verbund.de/carmentis/index.html*

mit einer frühen Warnung der Internet-Gemeinschaft eine Hilfestellung gibt. Allerdings werden zum Teil nicht so detaillierte Informationen zur Verfügung gestellt. Sie basieren zu einem großen Teil auf Statistiken über Portscans und Netzauslastungen und aktueller Meldungen über Schwachstellen (BugTraq).

Es existiert im Internet eine große Anzahl von kommerziellen sowie nicht-kommerziellen Anbietern mit sehr unterschiedlicher Qualität. Ein Vergleich und eine Bewertung der Dienste ist schwer möglich, da das wichtigste Kriterium fehlt, nämlich der Nachweis der Verhinderung oder Eindämmung einer Bedrohung.

Auf nationaler Ebene sind zwei Ansätze zu erwähnen, die Projekte „Internet Analyse System (IAS)“[3] und „CarmentiS“[4]. Beide Ansätze werden vom Bundesamt in der Informationstechnik (BSI) unterstützt.

Mit Hilfe des IAS werden Profile insbesondere der höheren Kommunikationsschichten erstellt. Durch Einsatz von Sonden, die an ausgesuchten Punkten des Internets platziert werden, wird der Kommunikationsverkehr analysiert. Mit den Ergebnissen des Internet-Analyse-Systems werden neue Informationen gewonnen, mit denen Trends über die Nutzung bestimmter Technologien erkannt, Zustände beobachtet und Probleme analysiert werden können.

Im Projekt „CarmentiS“ erproben Teams des deutschen CERT-Verbunds die Basisinfrastruktur für ein deutsches IT-Frühwarnsystem. Dieses soll zeitnah die Erkennung und Bewertung von akuten Bedrohungen erlauben. Zugleich dient CarmentiS als Testbed zur Erprobung neuer Ansätze und Strategien zur Visualisierung und automatischen Erkennung neuer Bedrohungen.

Beide Ansätze liefern erste Ergebnisse und Beiträge zur Lageeinschätzung.

Motivation für einen nationalen Ansatz

Das Internet kennt keine wirkliche nationale Ausprägung, sondern ist vielmehr ein echtes globales Medium, welches von breiten gesellschaftlichen Gruppen, der internationalen Industrie und Wirtschaft gleichermaßen genutzt wird. Aufgrund der IT- und Netzintegration in

wesentliche Prozesse des gesellschaftlichen Lebens und der Industrie besteht eine erhebliche Abhängigkeit vom Funktionieren des Internets, dessen eigener Sicherheit und der Sicherheit aller angeschlossenen Systeme. Auch wenn ein globaler Maßstab in der Nutzung und gleichermaßen der Sicherheit zugrunde liegt, gibt es dennoch Interessen und Bedürfnisse der handelnden Akteure, die sich regional, national und/oder hinsichtlich der Wirtschaftsräume unterscheiden können.

Denkbar ist, dass beispielsweise ein technologieführender Wirtschaftszweig eines nationalen Wirtschaftsraums zur Spielfläche von Konkurrenz- und Wettbewerbsspionage wird. Somit wären nicht nur wirtschaftliche Interessen von Unternehmen berührt, sondern ebenfalls nationale Interessen. Der Staat ist daher gefordert, einen Beitrag zum angemessenen Schutz des Wirtschaftsstandorts zu leisten.

Auch der BITKOM hat in einem Positionspapier[5] gefordert, dass alle im IT-Sicherheitsbereich tätigen Akteure eng kooperieren müssen: Sicherheitsbehörden, Strafverfolgungsbehörden, ITK-Hersteller und -Dienstleister, CERT-Verbünde und wissenschaftliche Einrichtungen. Das IT-Frühwarnsystem ist dann ein präventiv orientiertes Element im Rahmen eines Gesamtsystems, um zukünftige Angriffe rechtzeitig zu erkennen.

Win-Win-Situation

Ohne einen noch näher zu definierenden Aufwand hinsichtlich technischer, organisatorischer und personeller Mittel ist die Einrichtung eines IT-Frühwarnsystems nicht leistbar. Ebenfalls unabdingbar ist die vertrauensvolle Zusammenarbeit einer Reihe von Akteuren aus Industrie, Wirtschaft, gesellschaftlichen Gruppen und staatlichen Institutionen.

Um die einzelnen Akteure zu motivieren, sich an einem IT-Frühwarnsystem zu beteiligen, bedarf es ausreichender Anreize. Jedem einzelnen Akteur muss durch die konstruktive Mitarbeit in einem IT-Frühwarnsystem eine „Rendite“ zuteil werden, also mehr Gewinn bringen als eigener Aufwand zu investieren ist. Neudeutsch spricht man gerne von „Win-Win“-Situationen, die für alle beteiligten Akteure bei individuell unterschiedlichen Einsätzen einen Gewinn bringen. Dabei braucht das Renditemodell nicht rein finanziell orientiert sein. Wichtig ist, dass die Bedürfnisse und Interessen der Teilnehmer erfüllt werden. Ein Hauptargument für die „Sozialisierung“ der asymmetrischen Gefährdungssituation ist, dass auf Seiten der potenziellen Opfer eine schlagkräftigere Abwehrstrategie möglich wird.

Die bereits aufgeführten Projekte IAS und CarmentiS bieten entsprechende Kooperationsmodelle an.

Nachweis für das Funktionieren eines IT-Frühwarnsystems

Bei der Risikominimierung stehen komplementär auch andere präventive Sicherheitsmaßnahmen zur Verfügung, die in jedem Fall ergriffen werden sollten. So ist es heute immer noch so, dass durch ungepatchte Systeme und Schwachstellen in der Applikationsebene die größte Gefährdung ausgeht. Aber selbst wenn dieses durchgängig gemacht würde, ergäben sich noch immer viele Gefährdungen, die durch ein funktionierendes IT-Frühwarnsystem hoffentlich besser beherrscht werden könnten.

Bislang ist häufig die Behauptung aufgestellt worden, IT-Frühwarnsysteme könnten rechtzeitig vor neuen konkreten Gefährdungen warnen, sofern nur genügend Informationen und Daten für eine vorherige Auswertung und Analyse zur Verfügung stünden. Bis heute fehlt für diese Aussage aber noch ein formaler Beweis. Zugleich sollte jedoch klar sein, dass es niemals eine 100%ige aussagekräftige IT-Frühwarnung geben kann, da zu viele Unbekannte und aktive Teilnehmer im Spiel sind. So wird es sicherlich auch zu Fehlwarnungen kommen. Dieses wird von Gegnern eines IT-Frühwarnsystems immer ausgeschlachtet werden.

Ein IT-Frühwarnsystem muss neben den Daten aus Sensornetzwerken, Statistiken und automatisierten Log-Eventauswertungen auch Informationen aus sozialen Kontexten berücksichtigen. Des Weiteren ist für ein aussagekräftiges und funktionierendes System eine repräsentative Abdeckung von Informationssystemen der Akteure aus Wirtschaft, Wissenschaft und öffentlicher Hand sicherzustellen.

Die heute verfolgten Ansätze im Bereich IT-Frühwarnung konnten bereits Anomalien dem Ausbruch von Schadsoftware zuordnen (z. B. das IAS-System in Bezug auf „Sasser“). Diese A-posteriori-Betrachtungen müssen weiter ausgebaut werden. Es muss darum gehen, mithilfe der gesammelten Daten/Informationen im Vorlauf von bereits erfolgten IT-Angriffen die Muster von Angriffen im Nachhinein zu erkennen und dieses für die Zukunft anzuwenden. Letztlich sollte eine Aussage möglich sein wie: „Wenn folgende Daten/Informationen vor dem erfolgten Angriff auf folgende definierte Weise ausgewertet worden wären, hätte eine Information zur Vermeidung und/oder Milderung des Angriffs vorgelegen“. Je besser

[5] *http://www.bitkom.org/files/documents/Positionspapier_IT-FWS_in_Deutschland_V1.0f.pdf*

der Nachweis gelingt, umso größer wird die Motivation der unterschiedlichen Akteure zur Zusammenarbeit in einem nationalen IT-Frühwarnsystem sein.

Wirtschaftlichkeit

Bei allen Anstrengungen, die für den Aufbau eines IT-Frühwarnsystems unternommen werden, ist die Frage hinsichtlich der Wirtschaftlichkeit und Tauglichkeit zu stellen. Der Aufwand für ein IT-Frühwarnsystem wird mutmaßlich schnell steigen, ohne dass der Nachweis geführt werden kann, dass potenzielle Schäden verhindert worden sind. Wie so häufig, kann ein Return-On-Security-Investment im präventiven Sicherheitsmanagement nicht gerechnet werden, da für das Nichteintreten eines Schadens keine Daten über Größe, Ausmaß und Dauer vorliegen können.

Fazit

Wie der Weg zu wirksamen IT-Frühwarnsystemen aussehen wird, ist noch nicht abschließend geklärt. Bei allen Plänen und Maßnahmen muss man sich heute am Gesichtspunkt der Wirtschaftlichkeit und Tauglichkeit orientieren. Ohne den Nachweis beider Gesichtspunkte wird ein Frühwarnsystem nicht erfolgreich etabliert werden können.

Die Grundlage für das System, nämlich eine breite und intensive vertrauensvolle Zusammenarbeit vieler Akteure, wird nicht zustande kommen, wenn die Akteure selber nicht von der Sinnhaftigkeit überzeugt sind. Ohne breite Beteiligung ergibt sich kein Erfolg, ohne Erfolg ergibt sich keine breite Beteiligung von weiteren Akteuren. Aus diesem Grund ist es von immanenter Wichtigkeit, dass die heutigen Frühwarnsystemansätze schnell weitere Akteure und Teilnehmer finden.

TeleTrusT Deutschland wird sich hierbei stärker engagieren, da eine der größten Herausforderungen der nächsten Jahre für unseren Wirtschaftsstandort sein wird, wie wir die Vertrauenswürdigkeit und Verlässlichkeit moderner Informations- und Kommunikationsinfrastrukturen im globalen Wettbewerb bewahren und stärken können. *TeleTrusT* bietet sich hier als vertrauenswürdige und neutrale Plattform für weitere Gespräche und Aktivitäten in Bezug auf IT-Frühwarnung an. ■

Verschlüsselungslösungen für den Praxiseinsatz

Von

Dr. Volker Scheidemann
Leiter Produktmanagement beim
TeleTrusT-Mitglied Applied Security GmbH

Geradezu gebetsmühlenartig weisen IT-Sicherheitsberater und diverse Medien beim Thema IT-Sicherheit immer wieder – und völlig zurecht – darauf hin, dass eine Firewall und ein Anti-Virus-Programm noch keine sichere IT bedeuten. Viele extrem sicherheitskritische Vorfälle können weder von Firewall, noch von Virenscannern abgefangen werden. Die Serie von verlorenen Datenträgern mit Millionen von vertraulichen Personendaten, die letztens in Großbritannien Wellen bis in die höchsten politischen Kreise geschlagen hat, spricht eine deutliche Sprache und ist doch nur die Spitze des Eisbergs. Dennoch sind viele Verantwortliche nach wie vor auf dem Ohr taub, an das die IT-Administratoren ihre flehentlichen Wünsche nach IT-Sicherheitsmaßnahmen für den Einsatz innerhalb der durch die Firewall gegebenen Schutzmauer richten. Ihre Sorge um die Sicherheit der eigenen Daten bekommen Administratoren im Gegenteil häufig „gedankt" mit der latenten Unterstellung, sie könnten ihre Allmacht über die IT eines Unternehmens zum eigenen Vorteil ausnutzen und Daten einsehen oder manipulieren, die sie nichts angehen. Eine Möglichkeit, sowohl etwas für die Datensicherheit zu tun als auch dem Chef zu beweisen, dass man eben nicht in seinen Gehaltszettel schaut, ist der Einsatz einer Verschlüsselungslösung, bei der die Rollen der IT-Administration und der Sicherheitsverwaltung getrennt sind.

Verschlüsselung ist nicht gleich Verschlüsselung

Eine gute und praxistaugliche Verschlüsselungslösung ist mehr als eine Ansammlung von kryptografischen Algorithmen. Viel wichtiger ist, ob eine Lösung wirklich die Anforderungen für den praktischen Einsatz innerhalb eines Unternehmens erfüllt. Dies bedingt zunächst einmal, dass sich das Unternehmen darüber klar wird, was es eigentlich schützen will und vor wem. Es gibt unterschiedliche technische Ansätze bei Verschlüsselungen, die alle ihre Vor- und Nachteile haben und der Sicherheitsverantwortliche tut gut daran, die Unterschiede zu kennen. Je nach Anforderung kann nämlich mal die eine, mal die andere Lösung die bessere Wahl sein. Weiterhin muss zunächst geklärt werden, ob Kommunikationswege zwischen verschiedenen Standorten abgesichert werden sollen, in diesem Fall reden wir über E-Mail-Verschlüsselung oder über VPN, oder ob es sich um interne Sicherung von Datenbeständen handeln soll. Hier geht es dann um File/Folder-Encryption (FFE), Festplattenverschlüsselung oder Containerverschlüsselung. Über die ersten beiden Themen ist schon viel geschrieben und gesagt worden, wir wollen uns hier einmal auf das Thema „interne Sicherheit" konzentrieren.

Anforderungen für den Praxiseinsatz

Neben der in der Natur der Sache liegenden Forderung nach Sicherheit, stellen sich noch eine ganze Reihe anderer Fragen, die eine Verschlüsselungslösung beantworten muss, um für die Praxis tauglich zu sein. Auf der einen Seite steht die – ganz entscheidende – Frage nach der Nutzerakzeptanz. Als einziges, wirklich akzeptiertes Konzept hat sich hier die so genannte transparente Verschlüsselung durchgesetzt. Transparent bedeutet in dem Fall, dass der Benutzer überhaupt nichts von der Verschlüsselung mitbekommt, sie weder händisch anstoßen, noch sich darüber Gedanken machen muss, ob überhaupt verschlüsselt werden soll. Verschlüsselung darf keine gewohnten Arbeitsabläufe beeinträchtigen. Damit dies funktioniert, muss eine Lösung jedoch über eine zentrale Administration und über sinnvolle Identifizierungs- und Authentisierungsmechanismen verfügen, um berechtigte von unberechtigten Nutzern unterscheiden zu können. Damit sind wir bei der zweiten Hauptfrage, nämlich der nach der Administrierbarkeit der Lösung. Nichts ist so unsicher in der IT, vom Benutzer einmal abgesehen, wie eine falsch gewartete Sicherheitslösung. Als dritter wichtiger Punkt sollte die oben bereits angesprochene Rollentrennung zwischen IT und Sicherheitsverwaltung möglich sein, um die Verantwortung auf mehrere Schultern verteilen zu können, ohne jedoch die täglich notwendigen Arbeiten wie Backups und IT-Verwaltung zu beeinträchtigen.

Data Loss Prevention und Information Leakage Prevention

Unter den Begriffen Information Leakage Prevention (ILP) und Data Loss Prevention (DLP) verbergen sich neue Ansätze in der Entwicklung von Datensicherheitsprodukten, die über die reine Verschlüsselung hinaus gehen. Auch zum Umgang mit vertraulichen Daten berechtigten Personen soll es unter Umständen nicht erlaubt sein, diese Daten außerhalb der definierten Sicherheitsbereiche innerhalb eines Unternehmens zu benutzen. Bekanntester Typ von Software sind hier Port- oder Deviceblocker, welche den Abfluss von Daten über bestimmte Kanäle, z.B. USB-Schnittstellen, kontrollieren. Wünschenswert ist natürlich eine Konvergenz der Technologien Verschlüsselung und Devicekontrolle, nicht nur aus Kostengründen, sondern auch aus Gründen der einfacheren Handhabung, sowohl beim Ausrollen, als auch im laufenden Betrieb.

Eine Lösung für viele Ansprüche

Aus Anwendersicht ist eine Lösung wünschenswert, welche die Befriedigung vieler Ansprüche in einem Produkt vereint. Am Markt erhältlich sind diverse File & Folder-Verschlüsselungslösungen, die von der Papierform her dasselbe leisten, doch liegen bei genauerem Hinsehen teilweise große Unterschiede im Nutzen für den Anwender vor. Eine lange Featureliste macht noch nicht notwendigerweise ein gutes Produkt. Ein gutes Entscheidungskriterium, welches man bei der Auswahl einer Sicherheitslösung stets anlegen sollte, ist die Frage: Benötigt man eine Funktion wirklich dringend oder ist es lediglich in manchen Spezialfällen „nice to have“?

Bei den am Markt erhältlichen File & Folder-Verschlüsselungslösungen muss man zunächst unterscheiden zwischen rein clientbasierten Lösungen und Client-Server-Anwendungen. Die rein clientbasierten Lösungen benötigen für die Verwaltung der kryptografischen Schlüssel meist zusätzliche Datenbanken, z. B. MS SQL, welche hohe Zusatzanforderungen an Installation und Betrieb stellen. Außerdem sind rein clientbasierte Systeme in der Regel nicht in der Lage, schnell auf Änderungen der Verschlüsselungspolicy, z. B. den Entzug von Entschlüsselungsrechten für Benutzer, zu reagieren, da ein zentraler Server, welcher diese Information automatisch an die Clients verteilt, fehlt. Client-Server-Systeme haben den Vorteil, dass Konfigurations- und Schlüsselmanagement durch eine Serverkomponente automatisch erledigt werden und keine zusätzlichen Datenbanken benötigen. Die durch den Server – nennen wir ihn Security Server – gegebene zusätzliche Infrastrukturkomponente ist in der Regel kein Hinderungsgrund. Zur Sicherung der Ver-

fügbarkeit sollte der Security Server redundant ausgelegt werden (Master/Slave-Konzept) können. Die Verwaltung des Servers übernimmt der Sicherheitsverantwortliche meist mittels einer grafischen Benutzeroberfläche, welche remote auf den Security Server zugreift.

Vor dem Einsatz einer Verschlüsselungslösung sollte weiter geprüft werden, ob die Clientsoftware evtl. auf einem Terminalserver eingesetzt werden soll. Nicht alle marktgängigen Lösungen bieten hier Unterstützung. Wenn kein Terminalservereinsatz geplant ist, sondern die Clientsoftware auf verteilten Arbeitsplätzen eingesetzt werden soll, sollte auf jeden Fall eine zentrale Installation per Softwareverteilung möglich sein.

PKI oder nicht PKI – das ist hier nicht die Frage

Schlüsselverwaltung und Authentifizierung basieren in aller Regel auf Mechanismen der Kryptografie mit öffentlichen Schlüsseln (Public Key Cryptography) und benötigen für den sicheren Betrieb eine Public-Key-Infrastruktur (PKI). Eine gute Verschlüsselungslösung sollte sowohl out-of-the-box einsatzfähig sein, d. h. die nötigen PKI-Komponenten selbst mitliefern, als auch mit einer bereits bestehenden PKI – etwa einer Microsoft PKI – zusammenarbeiten können. Hierbei ist unbedingt darauf zu achten, dass eine Standardschnittstelle wie beispielsweise PKCS#11 für den Einsatz von Smartcards oder USB Kryptotokens unterstützt wird, damit man nicht eine unangenehme und teure Überraschung erlebt, wenn die Verschlüsselungssoftware nicht mit dem verwendeten Schlüsselmedium zusammenarbeitet.

Zur Reduktion des Aufwandes bei der Benutzerverwaltung ist es ein Muss, dass die Lösung sich an Verzeichnisdienste wie z. B. Microsoft Active Directory oder Novell eDirectory andocken kann und, dass diese Fähigkeit nicht erst als kostenpflichtiges Zusatzmodul erworben werden muss.

Zentrale Administration mit Rollentrennung

Werden Sie skeptisch, wenn der Anbieter einer Verschlüsselungslösung zusammen mit der Software gleich einen Workshop oder ein technisches Administratortraining mitverkaufen will! Eine gute und sichere Verschlüsselung zeichnet sich insbesondere dadurch aus, dass sie sich schnell und einfach installieren und zentral administrieren lässt. Sie sollten jederzeit in der Lage sein, die Verschlüsselungsregeln selbst festzulegen

---

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik (BSI) Halle 6, Stand K 30

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde am 1. Januar 1991 gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern. Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Als Behörde ist sie damit im Vergleich zu sonstigen europäischen Einrichtungen einzigartig. Derzeit sind dort fast 500 Informatiker, Physiker, Mathematiker und andere Mitarbeiter beschäftigt. Seinen Hauptsitz hat das BSI in Bonn.

Mit der rasanten Fortentwicklung der Informationstechnik entstehen in fast allen Bereichen des Alltags neue IT-Anwendungen – und damit auch immer neue Sicherheitslücken. Je abhängiger der Mensch von der Informationstechnik wird, desto mehr stellt sich die Frage nach deren Sicherheit. Unsere Gesellschaft ist stärker als zuvor durch Computerversagen, -missbrauch oder -sabotage bedroht. Bisher kann nicht ausreichend sichergestellt werden, dass die Informationstechnik das tut, was sie soll, und nichts tut, was sie nicht soll. Weil die Probleme in der Informationstechnik so vielschichtig sind, ist auch das Aufgabenspektrum des BSI sehr komplex: Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen. Es informiert über Risiken und Gefahren beim Einsatz der Informationstechnik und versucht Lösungen dafür zu finden. Dies beinhaltet die Prüfung und Bewertung der IT-Sicherheit von IT-Systemen, einschließlich deren Entwicklung in Kooperation mit der Industrie. Auch bei technisch sicheren Informations- und Telekommunikationssystemen können Risiken und Schäden durch unzureichende Administration und Anwendung entstehen. Um diese Risiken zu minimieren beziehungsweise zu vermeiden, wendet sich das BSI an eine Vielzahl von Zielgruppen: Es berät Hersteller, Vertreiber und Anwender von Informationstechnik. Darüber hinaus analysiert es Entwicklungen und Trends in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik

Postfach 200363
53133 Bonn
Telefon: 0228 99 9582-0
Telefax: 0228 99 9582-5400
Homepage: http://www.bsi.bund.de

und Ihrer Policy gemäß anzupassen, ohne auf das Know-how von Spezialisten zurückgreifen zu müssen. Es ist durchaus nicht nötig, dass eine Lösung von einem Sicherheitsadministrator Kenntnisse über Kryptografie oder Zertifikatsmanagement verlangt oder gar die Kenntnisse eines IT-Administrators, was Netzwerk- oder Benutzerverwaltung angeht. Auch Nicht-Techniker sollten die Rolle des Sicherheitsverantwortlichen übernehmen können, z. B. aus besonders kritischen Bereichen wie Revision oder Personalabteilung. Wichtig ist auch, dass Sicherheitsadministratoren mit Berechtigungsattributen versehen werden können, um ein Vier-Augen-Prinzip bei der Erstellung und Änderung von Regeln zu gewährleisten. Vor allem aber muss eine Verschlüsselungslösung gewährleisten, dass die Rollen von Sicherheitsadministrator und Systemadministrator getrennt werden können. Fragen Sie den Anbieter einer Verschlüsselung, wie genau das angebotene Produkt dies leistet!

Verschlüsselte E-Mail-Anhänge

Sehr nützlich ist es, wenn aus verschlüsselten Dateien automatisch verschlüsselte E-Mail-Anhänge erzeugt werden können, welche beim E-Mail-Empfänger über ein mitgeteiltes Passwort und evtl. mithilfe einer kostenlos zur Verfügung gestellten Software entschlüsselt werden können. Ein solcher Zusatznutzen ist nicht zu unterschätzen und löst eines der Hauptprobleme bei der Datenvertraulichkeit, denn häufig genug müssen sensible Dokumente auch mit Externen, z. B. Anwälten, Steuerberatern etc. ausgetauscht werden. Und dann hat man zwar eine sichere Ablage im eigenen Netz, reißt aber per E-Mail – weils ja so schön bequem ist – beim Versand eine riesige Sicherheitslücke auf. Glücklicherweise bietet der Markt auch hier Lösungen, die das beherrschen, wenngleich das bei weitem nicht alle sind, unabhängig vom Bekanntheitsgrad des Anbieters.

Notfallkonzept

Ein Recovery-Konzept für den Notfall ist ein Muss! Der Super-GAU der Verschlüsselung sind verschlüsselte Daten, an die auch der rechtmäßige Besitzer nicht mehr herankommt aufgrund von Schlüsselverlust o. Ä. Selbst im Fall eines Totalausfalls des Security-Servers oder einer anderen schlüsselverwaltenden Instanz, z. B. nach einem Brandschaden, müssen verschlüsselte Dateien noch entschlüsselt werden können. Eine im größeren Stil einsatzfähige Lösung muss hier eine schnelle und unkomplizierte Lösung bieten. Im Sinne der schnellen Datenverfügbarkeit und der Business Continuity ist eine solche Option unverzichtbar. ■

TeleTrusT Deutschland e. V.

www.teletrust.de

Vorstand

Vorsitzender:

Prof. Dr. Norbert Pohlmann
Fachhochschule Gelsenkirchen
Institut für Internet-Sicherheit – ifis
Neidenburger Straße 43, D-45877 Gelsenkirchen

Stellvertreter:

Michael Leistenschneider
DATEV eG
Paumgartnerstraße 6-14, D-90329 Nürnberg

Beisitzer:

Prof. Dr. Sachar Paulus
SAP AG
Dietmar-Hopp-Allee 16, D- 69190 Walldorf

Jürgen Sembritzki
Zentrum für Telematik im Gesundheitswesen GmbH
Campus Fichtenhain 42, D-47807 Krefeld

Geschäftsführung

Dr. Günther Welsch
Geschäftsführer
guenther.welsch@teletrust.de

Dr. Helmut Schütze
Referent
helmut.schuetze@teletrust.de

Marion Gutsell
Assistentin
marion.gutsell@teletrust.de

Kommunikation

Tel.: +49 30 2789 0362
Fax: +49 30 9789 4106
TeleTrusT Büro Berlin:
Chausseestraße 17
10115 Berlin

Pressekontakt

Sabine Faltmann
s.faltmann@faltmann-pr.de
Tel.: +49 24 1894 6822
Fax: +49 24 1894 6844
faltmann-PR
Kackertstraße 4
52072 Aachen

Ansprechpartner in den TeleTrusT-Themenbereichen

Kritische Infrastrukturen und Frühwarnsysteme
Dr. Günther Welsch, TeleTrusT Deutschland e.V.
guenther.welsch@teletrust.de

Personal Security Environment – PSE
Michael Hartmann, SAP AG
michael.hartmann@teletrust.de

Medizinische Anwendungen
einer vertrauenswürdigen Informationstechnik
Dr. Christoph Goetz, Kassenärztliche Vereinigung Bayerns
christoph.goetz@teletrust.de

Mobilität und Sicherheit – MuS
Stephan Wappler, IT-Services and Solutions GmbH
stephan.wappler@teletrust.de

Biometrische Identifikationsverfahren
Prof. Dr. Christoph Busch, CAST Forum e.V.
christoph.busch@teletrust.de

Public-Key-Infrastrukturen – PKI
Stephan Wappler, IT-Services and Solutions GmbH
stephan.wappler@teletrust.de

Onlineprozesse und Identitätsmanagement
Norbert Olbrich, RSA Security GmbH
norbert.olbrich@teletrust.de

SOA Security – Serviceorientierte Architektur Sicherheit
Dr. Bruno Quint, Corisecio GmbH
bruno.quint@teletrust.de

Elektronische Identitäten – eID
Prof. Dr. Helmut Reimer, Ehrenmitglied
von TeleTrusT Deutschland e.V.
helmut.reimer@teletrust.de

Torsten Wunderlich, DATEV eG
torsten.wunderlich@teletrust.de

OID (Object Identifier)
Dr. Helmut Schütze, TeleTrusT Deutschland e.V.
helmut.schuetze@teletrust.de

TISP
(TeleTrusT Information Security Professional)
Dr. Helmut Schütze, TeleTrusT Deutschland e.V.
helmut.schuetze@teletrust.de

European Bridge-CA (EB-CA)
Dr. Helmut Schütze, TeleTrusT Deutschland e.V.
helmut.schuetze@teletrust.de

Peter Steiert, NetSys.IT
peter.steiert@teletrust.de

Konferenzbeteiligungen:

RSA Conference in San Francisco,
7. bis 11. Apr. 2008
ISSE Conference in Madrid, 7. bis 9. Okt. 2008

Mitglieder bei *TeleTrusT* Deutschland e.V.

Stand: Februar 2008

ABDA – Bundesvereinigung Deutscher Apothekenverbände
Applied Security GmbH
Arendt Business Consulting
Atos Origin GmbH
AuthentiDate International AG
BCC Unternehmensberatung GmbH
bos bremen online services
Brainloop AG
Bromba GmbH
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bundesdruckerei GmbH
Bundeskriminalamt Wiesbaden
Celectronic GmbH
Cherry GmbH
Cognitec Systems GmbH
Computer-Communication Networks GmbH
Corisecio GmbH
Cross Match Technologies GmbH
DATEV eG
DE-CODA GmbH
DERMALOG Identification Systems GmbH
Deutsche Bank AG
Deutscher Genossenschafts-Verlag eG
Deutscher Sparkassen Verlag GmbH
DFN – Deutsches Forschungsnetz e.V.
DGN Deutsches Gesundheitsnetz Service GmbH
Dr. Fehr GmbH
D-Trust GmbH
ekey biometric systems Deutschland GmbH
Fachhochschule Gelsenkirchen
Fraunhofer Institut für Biomedizinische Technik
Fraunhofer Institut für Graphische Datenverarbeitung
Fraunhofer Institut für Sichere Informationstechnologie
GAD – Gesellschaft für automatische Datenverarbeitung eG
Gemalto GmbH
Giesecke & Devrient GmbH
Hasso-Plattner-Institut an der Universität Potsdam
Humpert Consulting GmbH
IICS GmbH
INFORA GmbH
International School of IT-Security - gits AG -
ITSG – Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH
Kassenärztliche Bundesvereinigung
Kassenärztliche Vereinigung Bayerns
Kassenzahnärztliche Bundesvereinigung
Kobil Systems GmbH
media transfer AG
Microsoft Deutschland GmbH
NEC Deutschland GmbH
NetSys.IT GbR
NEXUS Technology GmbH
Nimbus Technologieberatung
NXP Semiconductors Germany GmbH
OMNIKEY ERFURT
PAV Card GmbH
PGP Deutschland AG
PVS – Verband der Privatärztlichen Verrechnungsstellen
ROHDE & SCHWARZ SIT GmbH
RSA Security GmbH
SAP AG Technology Development
SCM Microsystems GmbH
Secorvo Security Consulting GmbH
secrypt GmbH
Secude IT Security GmbH
secunet AG
Siemens AG
SignCard GmbH & Co. KG
SOFTPRO GmbH
TC TrustCenter GmbH
Teleca Systems GmbH
THALES e-TRANSACTIONS GmbH
Totemo AG
T-Systems Enterprise Services GmbH
TÜV Informationstechnik GmbH
Utimaco Safeware AG
Zentrum für Telematik im Gesundheitswesen GmbH

Assoziierte Mitglieder

AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.
CAST Forum e.V.
COMPUTAS G. Geuhs GmbH
GDD e.V.
SILICON TRUST
VOI – Verband Organisations- und Informationssysteme
VSWM – Verband für Sicherheit in der Wirtschaft in Mitteldeutschland

Ehrenmitglieder

Dietrich Kruse
Dr. Karl Rihaczek
Prof. Dr. Helmut Reimer