

## **Ist Ihre Identität wirklich sicher?**

### **Schutz vor „Identitätsdiebstahl“ durch Datenverschlüsselung**

*Von Tom de Jongh, Product Manager bei SafeBoot*

„Identitätsdiebstahl“, also die missbräuchliche Nutzung personenbezogener Daten durch Dritte, ist eine immer größer werdende Bedrohung. Laut einer aktuellen Studie von McAfee ist jeder vierte Anwender diesem hohen Risiko ausgesetzt. Wertvolle Informationen werden im Unternehmen immer häufiger zentral gespeichert und verwaltet. Dabei wissen die Mitarbeiter oftmals gar nicht, wo sich diese befinden. Viel zu häufig sind diese Daten nicht sicher und unberechtigte Personen können darauf zugreifen – beispielsweise durch Hackangriffe auf das Netzwerk oder aber Backupplatten, Rechner oder Laptops werden gestohlen. In Folge werden persönliche Daten wie z. B. Kreditkartennummern auf einen Blick bekannt. In den USA hat Identitätsdiebstahl bereits massive Ausmaße angenommen. Dort ist vor allem die Sozialversicherungsnummer ein begehrtes Objekt der Betrüger.

#### **Sicherheitsbrüche**

Eines der Aufsehen erregendsten Diebstähle vertraulicher Daten fand im Juni 2005 bei einem Angriff auf CardSystems statt, einer Drittanbieter-Abrechnungsstelle für Transaktionen, die zur Begleichung von Kreditkarteneinkäufen Geld zwischen Banken überweist. Ein Hackerangriff auf das Netzwerk betraf weltweit über 40 Million Kundenkonten von verschiedenen Kreditkartenanbietern, darunter Visa und MasterCard. Unglücklicherweise finden diese Sicherheitseinbrüche laufend statt, wenngleich in kleinerem Umfang und auf mehr regionaler Ebene.

#### **Ist Identitätsdiebstahl eine neue Erscheinung?**

Identitätsdiebstahl ist nicht etwas, das erst vor kurzem in die Schlagzeilen gelangte und von den Medien hochgespielt wird. Dazu einige Zahlen :

- Nach Angaben der U.S. Federal Trade Commission (FTC) ist Identitätsdiebstahl die Nummer eins bei den Verbraucherbeschwerden – mit 42 Prozent aller Beschwerden im Jahre 2001.

- Im Januar 2001 berichtete CBSnews.com: „Alle 79 Sekunden wird eine „Identität gestohlen“, ein Konto im Namen des Bestohlenen eröffnet und der Dieb geht damit auf Einkaufstour.“

Dies geht also bereits seit geraumer Zeit so. Wie ist dies möglich?

Die Vorstellung der „sicheren Schutzzone“

Die rasante Verbreitung des Internets erfordert ein neues und erweitertes Sicherheitsdenken und –bewußtsein. Aber bis heute sind sich die Anwender großteils nicht im Klaren darüber, wie groß die Bedrohung durch Identitätsdiebstahls tatsächlich sein kann oder dass Eindringlinge weltweit versuchen, Zugriff auf personenbezogene Informationen zu erhalten.

Die meisten Menschen wissen, dass das Internet einige Sicherheitsrisiken birgt. Dies ist der Grund, warum Anwender und Unternehmen Virens Scanner auf PCs und Netzwerken installieren. Darüber hinaus wird mit Firewalls verhindert, dass sich Trojaner in das Netzwerk einschleichen, während VPNs (Virtual Private Networks) sicherstellen, dass vom Laptop oder dem PDA über das Internet gesendete Informationen an ein Unternehmensnetzwerk sicher sind.

Anwender und Unternehmen erstellen scheinbar undurchdringliche „Wände“ um ihre Netzwerke und Maschinen, so dass von außen keine unberechtigten Anwender hereinkommen können. Dies könnte man als Vorstellung einer „sicheren Schutzzone“ bezeichnen. Aber garantiert dieser Ansatz, dass sensitive Daten wirklich sicher sind?

Was passiert, wenn ein unberechtigter Benutzer die Schutzzone eines Anwenders oder eines Unternehmens durchbricht? Eine einzige Sicherheitsverletzung kann möglicherweise das gesamte Netzwerk und alle darin gespeicherten Daten offen legen. Ein „Trojaner“ sucht nach wertvollen Anwenderdaten und kann sich unbegrenzt im Netzwerk ausbreiten. In dem bei CardSystems erfolgten Einbruch wurden beispielsweise Informationen aus der Datenbank entwendet, indem dazu ein einfaches Skript ausgeführt wurde.

Einbrüche in die Sicherheitszone von Anwendern und Unternehmen durch Hackangriffe wie im Fall von CardSystems sind weithin bekannt. Es gibt aber weitere Sicherheitsrisiken durch Identitätsdiebstahl und die entsprechenden Methoden, die sensitive Daten gefährden.

*Peer-to-Peer* Lösungen zur gemeinsamen Nutzung von Informationen, wie Kazaa, können sensitive Informationen offen legen, da Festplatten- oder auch Netzwerke gemeinsam von den Teilnehmern über das Internet genutzt werden. Natürlich werden die Ports, die Kazaa verwendet, von der Unternehmens-Firewall blockiert, die diese Bedrohung größtenteils ausschaltet. Aber, was geschieht, wenn ein Anwender Daten auf einem Laptop oder einen Rechner zu Hause kopiert und Peer-to-Peer-Programme zu Hause auf einem mit dem Internet verbundenen Rechner ausführt?

Das Kopieren von Informationen von einem „sicheren“ Netzwerk auf *mobile Geräte*, wie Laptops und entfernbaren Speichermedien ist eine weitere Möglichkeit, d. h. Daten unabsichtlich unberechtigten Zugriffen auszusetzen. Zu diesen Speichermedien mit hohem Sicherheitsrisiko zählen Laptops, USB-Sticks sowie CDs oder DVDs. Mittlerweile haben diese Geräte enorme Speicherkapazitäten.

### **Was ist zu tun? Gibt es eine allgemeingültige Antwort auf Identitätsdiebstähle?**

Die Antwort ist ganz einfach. Es müssen die sensitiven Daten gesichert werden, anstatt lediglich das Netzwerk, die einzelnen Rechner oder die externe Festplatten zu schützen, auf denen sich die Daten befinden. Dazu gibt es verschiedene Wege. Beispielsweise Strategien, die Anwendern vorgeben, Daten nicht auf bestimmten Bereichen eines Netzwerks oder auf mobilen Geräten oder Home Computern zu speichern. Dabei ist die Entscheidung aber dem Endanwender überlassen und kann die alltäglichen Tätigkeiten des Anwenders einschränken. Also keine gute Wahl, da die Erfahrung zeigt, dass diese Lösung weder vertrauenswürdig noch wirksam ist.

Ein effektiverer Weg, sensitive Daten zu schützen, ist die contentbasierte Encryption, d. h. die Verschlüsselung der Inhalte. Wenn richtig konzipiert und implementiert wird, werden sehr effektiv geschützt und gleichzeitig werden aber die normalen Tätigkeiten des Anwenders nicht beeinträchtigt. Und sogar noch wichtiger, diese Methode unterstützt Richtlinien für Endanwender, die die Einhaltung gesetzlicher Bestimmungen sicherstellen.

### **Wichtige Überlegungen**

Bei der Auswahl und Implementierung einer contentbasierten Lösung zu Datenverschlüsselung sollten folgende Gesichtspunkte berücksichtigt werden:

- Persistenz und Transparenz

Es ist sehr wichtig, dass die Endanwender bei der Ausführung ihrer Tätigkeiten nicht behindert werden. Mit der Persistent Encryption Technology (PET) ist dies möglich. Wichtige Elemente dieser Technologie sind:

- **„On-the-Fly“ Verschlüsselung und Entschlüsselung:** Dateien und Verzeichnisse werden ohne Anwendereingriff verschlüsselt und entschlüsselt. Die Effizienz der Verschlüsselungstechnologie ist der Schlüsselfaktor für das reibungslose Arbeiten der Anwender.
- **Transparenz für Endanwender:** Wenn die Berechtigung der Endanwender für das System geprüft ist, sollten sie auf alle ihre Dateien und Ordner zugreifen können, ohne dass für jeden Zugriff Passwörter eingegeben werden müssen. Auf diese Weise ist keine Schulung der Endanwender erforderlich.
- **Verschlüsselung ist an Dateien und Ordner gebunden:** Dies stellt sicher, dass Daten immer sicher sind, egal wann und wo sie gespeichert wurden, so dass es für den Anwender nicht wichtig ist, wo die Daten gespeichert sind.

### **Ein zentralisiertes Management**

Ein Netzwerk besteht normalerweise aus zahlreichen Clients und Rechnern. Dazu bestehen Richtlinien, was Anwendern erlaubt ist und was nicht. Die Umsetzung dieser Richtlinien und das Management der sich ständig ändernden Richtlinien sollte zentral umgesetzt werden. Nur so werden die Anforderungen an die Administratoren und Gesamtbetriebskosten (TCO) reduziert.

### **Anbindung an Unternehmenssysteme**

Eine contentbasierte Verschlüsselungslösung ist wahrscheinlich nicht die einzige Sicherheitslösung, die im Unternehmen existiert. Ein einziger Administrationspunkt und eine einzige „Identität“ (d. h. Single Sign-On - nur ein Nutzernamen und nur ein Passwort - zusammen mit Smart Cards oder Tokens) für jeden Anwender und jedes System sind der Schlüssel. So können Anwender zufriedengestellt werden und Gesamtbetriebskosten gering gehalten werden. Sehr wichtig sind daher Verbindungen zu bestehenden Identitätsmanagementsystemen wie Microsoft Active Directory®, Microsoft PKI und Entrust PKI.

### **Sichere Datenwiederherstellung**

Schließlich müssen Daten vor unberechtigten Personen geschützt werden – jederzeit und an jedem Ort. Was passiert zum Beispiel, wenn ein Anwender sein Passwort oder seine Smart Card vergisst und eine wichtige Präsentation in Japan geben muss, aber nicht auf seine

Präsentationsdatei zugreifen kann? Es ist das oberste Gebot, Wiederherstellungsverfahren zu haben, die die Verfügbarkeit der Daten zu jeder Zeit und an jedem Ort sicherstellen.

Challenge/Response-Verfahren, sichere Authentifizierungsverfahren eines Teilnehmers, sind bewährte Vorgehensweisen für die Wiederherstellung von Daten.

Quellen:

<http://www.standaard.be/extra/geldzaken/index.asp?articleID=GE8FQ5J5>

<http://www.planet.nl/planet/show/id=67782/contentid=592407/sc=58eb98>

<http://www.securityfocus.com/news/11219>

<http://www.burger.overheid.nl/nieuws/?id=639>

<http://www.identity-theft-protection.com/stats.html>

[http://searchstorage.techtarget.com/originalContent/0,289142,sid5\\_gci1085051,00.html?bucket=NEWS](http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci1085051,00.html?bucket=NEWS)