

Daten sicher übermitteln

Menschliches Handeln technisch korrigieren

(BS/fra) Es wird viel über die Datensicherheit philosophiert. In fast allen Fällen spielt aber die sichere Datenübertragung eine herausragende Rolle, sei es nun beim elektronischen Personalausweis (ePerso) oder dem Einheitlichen Ansprechpartner. Schließlich müssen etwa die online übermittelten Daten und Freigaben des ePersos während der Transaktion so geschützt sein, dass kein Unbefugter sie abfangen und dann als eigene Identität nutzen kann. Hier kann nur die verschlüsselte Übermittlung Abhilfe schaffen.

Bei der Verschlüsselung werden die sogenannten Klardaten wie etwa das Geburtsdatum oder ein Passwort in eine unleserliche Zeichenfolge umgewandelt, die nur mit einem feststehenden "Schlüssel" wieder in Klartext umgewandelt werden können. Während es zwar die verschiedensten Modi gibt, kommt im Behördenbereich hauptsächlich die Ende-zu-Ende-Verschlüsselung zur Anwendung. Hierbei werden die Daten vom Anwender in ein verschlüsseltes Paket umgewandelt, das dann nur vom Empfangsrechner wieder entschlüsselt werden kann. Die Unsicherheit besteht in diesem Fall allerdings auf Seiten des Nutzers. Schließlich kann kein Beamter wissen, ob der Bürger etwa einen Virenschutz auf seinem PC installiert hat, ihn auch aktuell hält und des weiteren noch die herausgegebenen Sicherheitspatches installiert. Zudem könnte der Bürger noch ein häufiger Besucher von "unsicheren" Webseiten sein und dementsprechend über einen stark verseuchten Computer verfügen.

Um all diese Risikofaktoren zumindest etwas zu minimieren, soll das Paket zum ePerso auch einen kostenlosen Virenschutz enthalten. Allerdings ist auch das Verschenken der Sicherheit kein Garant für einen virensicheren PC. Doch was passiert nun, wenn der Nutzer den Schlüssel auf einem verseuchten Computer nutzt. Eine Forderung an das Verschlüsselungssystem beinhaltet dementsprechend einen pro-Aktiven Selbstschutz. Hierbei könnten unbefugte

Zugriffsversuche oder verdächtiges Verhalten von installierten Programmen zur Deaktivierung der Verschlüsselungsfunktion führen, sodass die Daten zumindest nicht in ihrer kodierten Form an Unberechtigte gelangen könnten.

Jede Sicherung ist zudem nur so gut wie das genutzte Passwort. Diese Binsenweisheit stellt in der Realität allerdings das größte Problem dar, weil Computer mittlerweile zu geübten Paßwortknackern geworden sind. Selbst der 256Bit-Schlüssel, also eine Folge aus 256 Zeichen, ringt den Maschinen nur paar Stunden Arbeit ab, Tendenz sinkend. Dem menschlichen Gehirn sind hingegen Grenzen gesetzt.

Die Verschlüsselung muss also neue Wege gehen, weg vom gemerkten Passwort hin zu technischen Methoden, um die Sicherheit der Daten weiterhin zu gewährleisten. Dementsprechend baut auch die angedachte Hardware zum elektronischen Personalausweis auf einen Fingerabdruckscanner, mit dem sich der Nutzer im Web identifizieren kann. Andere Methoden setzen auf elektronische Schlüssel, welche auf einem mobilen Gerät gespeichert sind. Der Nutzer muss sich also nicht mehr das Passwort merken, sondern nur noch seinen USB-Stick finden, der dann den Computer oder Laptop freischaltet. Bei allen Verschlüsselungsmethoden und -problemen bleibt der Faktor Mensch die größte Ungewissheit – und diese wird angesichts von über 80 Millionen potenziellen Nutzern nicht geringer.

Bedrohung durch Mobilfunk-Spione ernst genommen

Bundesinnenministerium ordert Krypto-Handys

(BS/leh) In der September-Ausgabe informierte der Behörden Spiegel über die zunehmenden Bedrohungsszenarien beim Umgang mit Mobilfunk und über die in diesem Zusammenhang vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene Sicherheitswarnung. Konsequenterweise steht das Bundesministerium des Innern inzwischen mit der Düsseldorfer Secusmart GmbH kurz vor Abschluss eines Rahmenvertrags für die Beschaffung von Krypto-Mobiltelefonen.



Dr. Hans-Christoph Quelle, Geschäftsführer von Secusmart, bei der Übergabe der symbolischen Smartcard an Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnologie (v.l.n.r.).

Foto: BS/Secusmart

Die mit Mitteln des Konjunkturprogramms finanzierten handelsüblichen Geräte sind mit einer microSD-Karte (Secusmart Security Card) ausgestattet, die eine vom BSI für VS-NfD zugelassene Sprachverschlüsselung ermöglicht. Gleichzeitig ist die Lösung Secuvoice zugelassen für die Geheimhaltungsstufe NATO restricted. Die von Secusmart entwickelte Lösung zur Sicherung der Mobilkommunikation basiert auf sichere vom BSI überprüfter Hardware, wobei al-

le sicherheitskritischen Funktionen gekapselt sind. Das heißt, dass alle Algorithmen für den Schlüsseltausch und das Schlüsselmanagement sowie der Verschlüsselungsalgorithmus selbst manipulationssicher sind. Sie laufen vollständig gekapselt innerhalb der sicheren Hardware und können nicht ausgespäht werden. Die komplette Sicherheitsanwendung wurde vom BSI entwickelt. Das gleiche Verfahren wird auch für die Ende-zu-Ende-Verschlüsselung im TE-

TRA-Netz der deutschen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) verwendet. Ver- und Entschlüsselung eines Gesprächs finden ausschließlich im Mobiltelefon innerhalb des Krypto-Controllers statt.

Dadurch sind die Gespräche sowohl auf der Luftschnittstelle als auch im Festnetz abhörsicher. Die Verschlüsselung erfolgt auf der Basis des 128-BIT AES (Advanced Encryption Standard). AES-128 ist von der NATO zugelassen für die Verschlüsselung von Gesprächen mit der Geheimhaltungsstufe NATO-Secret. Die notwendige Schlüsselvereinbarung zwischen Gesprächsteilnehmern läuft auf der Basis einer Variante der Elliptischen Kurven Kryptographie des Diffie-Hellmann Protokolls (ECDH) mit höchster Sicherheit und benötigt weniger als vier Sekunden. Darüber hinaus wird zur Sicherung der Kommunikation der nicht transparente GSM-CSD-Kanal verwendet. In Sachen Sprachqualität ist kein Unterschied zwischen einem sicheren und einem offenen GSM-Gespräch feststellbar. Die Sprachqualität bleibt auch bei einem verschlüsselten Gespräch auf gewohnt hohem Niveau, weil für die Sprachübertragung der original GSM-AMR-Sprachcodex verwendet wird.

Zur Abwehr von "Man-in-the-Middle-Angriffen" werden die zwischen den Gesprächsteilnehmern mittels ECDH ausgetauschten Schlüssel authentisiert. Zur Authentisierung der Schlüssel werden digitale Zertifikate als Teil einer Public Key Infrastruktur (PKI) verwendet. Für Behörden wird die PKI ausschließlich vom BSI verwaltet, das für die

Beschaffung, Personalisierung und Schlüsselverwaltung verantwortlich ist. Für kommerzielle Unternehmen fungiert Secusmart als Root-CA. Technische Unterschiede bestehen nicht. Jeder Krypto-Controller enthält ein Zertifikat, in dem der öffentliche Schlüssel und die kryptografische Identität des Nutzers durch die digitale Signatur der Root-CA unfälschbar miteinander verbunden sind. Das Zertifikat wird während der Produktion in den Krypto-Controller der Secusmart Security Card eingebracht und ist dort sicher gespeichert.

Die Secusmart Security Card wird in das normale Mobiltelefon gesteckt. Sie schränkt die üblichen Funktionen des Telefons in keiner Weise ein, sorgt für sicheres Telefonieren und – besonders wichtig – fällt nicht auf.

Das Bundesinnenministerium hat sich mit seiner Wahl für eine Lösung entschieden, bei der die mobile Kommunikation auf zweifache Weise "Ende-zu-Ende-Verschlüsselung und Authentifizierung der Gesprächsteilnehmer" gesichert wird und die in Bezug auf Benutzerfreundlichkeit, Sprachqualität und Sicherheit ihres Gleichen sucht. Nun bleibt nur noch abzuwarten, wie viele der Geräte von den Bundesbehörden abgerufen werden.

Secusmart arbeitet zur Zeit mit ausgewählten Behörden an einer Lösung für eine sichere mobile E-Mail-Kommunikation und wird mit der nächsten Version von Secuvoice ebenfalls die Kommunikation mit Satellitentelefonen sowie das sichere Empfangen und Versenden von SMS möglich machen.

Outsourcing in Kommunen

Zuverlässige Überwachung der Remote-Zugriffe

(BS) Outsourcing ist schon seit Längerem kein ausschließlich auf die Privatwirtschaft beschränktes Thema mehr. Im Hinblick auf nachhaltige Kostensenkungen entscheiden sich zunehmend auch Bundes-, Landes- und Kommunalbehörden für die Einführung von Outsourcing-Lösungen: von der Übertragung des IT-Betriebs an externe Dienstleister bis hin zur Auslagerung ganzer Verwaltungsprozesse. Die Sicherheit muss dabei natürlich an oberster Stelle stehen. Ein Bereich, der hier oft vernachlässigt wird, sind Zugriffe auf privilegierte Benutzerkonten, wie sie IT-Administratoren besitzen.



Die Aufzeichnungen werden in einem digitalen Tresor gespeichert.

Collage: BS/Liesegang

Privilegierte Benutzerkonten ermöglichen einen problemlosen Zugriff auf alle Datenbestände. Die Überwachung dieser Zugänge ist in vielerlei Hinsicht komplex; gerade dann, wenn der Administrator von außerhalb der Behörde eine Verbindung mit wichtigen Systemen aufbaut. In diesem Fall ist nicht nur zu kontrollieren, "Wer" dahinter steckt, sondern auch, "Was" Inhalt solcher Sessions ist.

Remote-Zugriffe sind in den meisten Behörden an der Tagesordnung. Ob bei Outsourcing, Outtacking oder im Supportfall: immer wieder ist es erforderlich, dass sich Spezialisten auf den Servern und Datenbanken einloggen oder eine Verbindung mit einer speziellen Verwaltungssoftware aufbauen; zum Beispiel, um Routineaufgaben zu erledigen oder zur Fehlerdiagnose und

-behebung. Doch wer ist es, der da an Systemen mit vertraulichen Informationen arbeitet, und wie kann man sicher sein, dass nur die notwendigen und wirklich beabsichtigten Tätigkeiten durchgeführt werden?

Aktuelle Nachrichten zeigen zudem deutlich, wie einfach es ist, über die Nutzung privilegierter Zugänge auch weniger "ehrenhafte" Dinge anzustellen, und dass dabei so mancher Super-User der Verlockung erlegen ist, sich sensible Informationen zu verschaffen.

Wie bekommt man diese Situation in den Griff? Eine Lösung bietet Cyber-Ark mit dem Privileged Session Manager, mit dem gerade diese "mächtigen" Benutzerkonten – auch bei einem externen Zugriff auf IT-Systeme – zuverlässig gesichert und überwacht werden. Mit der Lösung

kann nicht nur überprüft werden, wer Zugang zu sensiblen Informationen hat, sondern auch, was er mit diesen Informationen macht. Es erfolgt eine komplette Aufzeichnung der Admin-Sessions und damit eine jederzeitige Nachvollziehbarkeit, was in ihnen konkret passiert ist.

Der Privileged Session Manager Proxy, über den die Verbindung zum Zielsystem automatisch aufgebaut wird, kann wie mit einem Digitalrecorder alle Aktionen vom Zeitpunkt der Anmeldung am System bis zur Abmeldung revisionssicher aufzeichnen.

Dies wird gerade bei Remote-Zugängen oder Outsourcing-Lösungen für viele Behörden nicht zuletzt aufgrund aktueller gesetzlicher Anforderungen und Compliance-Vorschriften von zunehmend größerer Bedeutung.

Alle Aufzeichnungen werden im AVI-Format in einem "virtuellen Tresor" archiviert, dem Digital Vault Server von Cyber-Ark. Sie können nur von berechtigten Personen abgerufen und eingesehen werden. Ein weiteres Sicherheitsmerkmal der Lösung ist, dass externe Dienstleister oder Administratoren Passwörter nie einsehen können.

Der Privileged Session Manager ist Bestandteil der Privileged-Identity-Management-Suite von Cyber-Ark, mit der privilegierte Benutzerkonten zentral verwaltet und überwacht werden können – einschließlich von Administrator-Passwörtern, die sich auf einem Router, Server, einer Workstation oder in einer Datenbank befinden, und von Passwörtern in Skripten oder Config-Files. Die Lösung lässt sich problemlos in bestehende Systeme integrieren und kann Hunderttausende von Passwörtern in heterogenen IT-Umgebungen sichern und verwalten.

PITS 2009

Kongress Public IT-Security

Kongress der Behörden Spiegel-Gruppe

ENTER PITS 2009!

27. Oktober 2009 im dbb forum berlin

Melden Sie sich jetzt an zu dem IT-Sicherheits-Event des Jahres speziell für den öffentlichen Sektor.

Als Treffpunkt der IT-Verantwortlichen in den Behörden von Bund, Ländern und Kommunen, der Anbieter von Sicherheitslösungen und der Wissenschaft gibt PITS wichtige thematische Impulse, dient dem Informationsaustausch und der Netzwerkbildung.

Themen sind u.a.:

- ▷ IT-Sicherheitsstrategien für Behörden,
- ▷ Authentifizierung und Identitäts-Management,
 - ▷ E-Mail Sicherung und Management,
 - ▷ BSI-Grundschutz, Auditing und Revision,
- ▷ Access Control – Sicherer Zugriff auf Netzwerke und Datenbanken,
 - ▷ Sichere mobile Kommunikation.

Auf der IT-Sicherheitsausstellung erfahren Sie alles über die neuesten Trends bei IT-Sicherheitsanwendungen: ob Managed E-Mail Security, Authentifizierungs- und Zugangsmanagement, Antivirus- und Antispam-Lösungen oder mobile IT-Sicherheit. 40 Aussteller präsentieren ihre Sicherheitslösungen auf der größten kongressbegleitenden Fachausstellung speziell für den Öffentlichen Dienst im Bereich IT-Sicherheit.

Weitere Informationen, das detaillierte Programm und die Anmeldung finden Sie unter www.public-it-security.de