Nr. 1, Januar 2011

ISSN 1862-4375

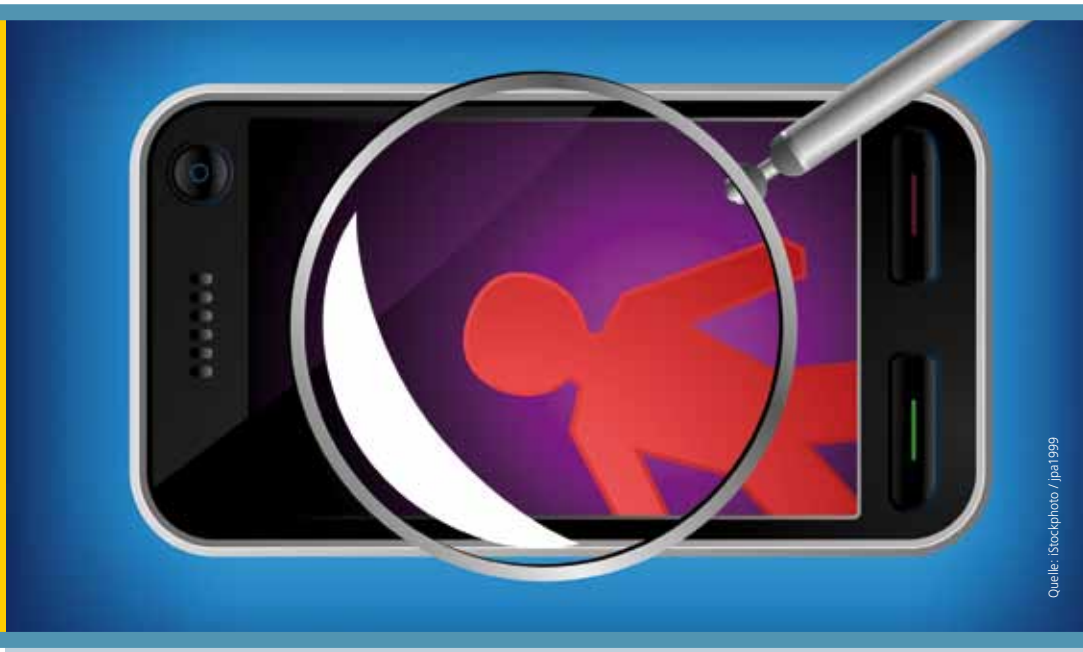
IT·Grundschutz

Informationsdienst

Studien und Analysen

Sicherheitsrisiko Smartphones

Seite 5



Quelle: iStockphoto / jpa1999

NEWS

Rubriken

IT und Recht

Studien und Analysen

Praxis und Anwendungen

Workshops

SecuMedia
Der Verlag für Sicherheits-Informationen

Mobile Computing

Smarte Handys gegen Hacker

Handys als Token nutzen

Manipulationssicher und vom Anwender akzeptiert: Smartphones machen auch als Security-Hardware Karriere.
Quelle: VASCO

Jan Valcke, President und COO, Vasco Data Security

Beim Telebanking wie im Geschäftsleben sind starke Authentisierung und digitale Signatur wichtiger denn je. Dabei kann das Mobiltelefon als Sicherheits-Hardware eine immer größere Rolle spielen. Die universell verbreiteten und akzeptierten Endgeräte bilden einen unabhängigen Informationskanal, der Hacker und Cracker außen vor lässt.

Wenn es um das Internet geht, rangieren die Reaktionen je nach Altersgruppe und Technikaffinität zwischen Begeisterung und verhaltener Ablehnung. Berufsbedingt sieht Jörg Ziercke, Präsident des Bundeskriminalamtes, das World Wide Web vor allem als Tatwerkzeug: „In immer mehr Kriminalitätsbereichen verwenden Betrüger das Internet“, so sein Resümee. Bereits 2009 musste die polizeiliche Kriminalstatistik rund 207.000 Fälle mit dem Tatmittel Internet registrieren, Tendenz steigend, nicht nur quantitativ, sondern auch qualitativ. „Die im Cybercrime aktiven Täter sind höchst innovativ, flexibel und reagieren auf neue Sicherungstechniken mit neuen oder angepassten Begehungsweisen“, sorgt sich Ziercke.

Die Sorge ist nicht unbegründet: An die 15 Millionen Euro Schaden allein beim Online-Banking erwarten das BKA und der Branchenverband BITKOM für 2010. Dieser klar zu beziffernde finanzielle Verlust dürfte allerdings nur die Spitze des Eisbergs sein. Der Schaden durch Informationsmissbrauch ist nach wie vor kaum abschätzbar. Ein besonders plakatives Beispiel sind zurzeit die vielen Tausend veröffentlichten Diplomaten-Depeschen auf Wikileaks, die zeigen, dass Datenverluste auch in eigentlich gut gesicherten Umgebungen möglich sind.

Das Grundprinzip: Identitätsmissbrauch

Die Methoden der Schattenwirtschaft werden in der Tat immer raffinierter. Analysiert man aber das Grundprinzip, so ergibt sich stets ein- und dasselbe Muster: Ganz gleich, ob Man-in-the-Middle-Angriff, Spear-Phishing-Attacke oder einfacher Keylogger, immer geht es darum, Menschen oder Maschinen eine andere Identität vorzugaukeln.

Dabei erweisen sich PC und Internet nach wie vor als geradezu ideale Hilfsmittel. Das Netz der Netze ist nun einmal in erster Linie auf freien Informationsfluss und Anonymität ausgelegt und weniger auf eindeutige Identifikation. Das Internet von heute bietet eine Unmenge nützlicher Programme, Applets und Downloads, die oft und gerne genutzt werden. Dass sich dabei immer wieder Malware auf die Rechner einschleicht, ist auch bei umsichtiger Nutzung schwer zu vermeiden. Sage und schreibe 43 Prozent aller Internet-Nutzer ab 14 Jahren haben schon einmal die Erfahrung gemacht, dass ihr PC infiziert war, wie eine Studie des BITKOM ergab. „Schadprogramme können nicht nur Rechner lahmlegen, sondern spähen vermehrt digitale Identitäten aus“, warnt BITKOM Präsidiumsmitglied Prof. Kempf. Etwa sieben Prozent der repräsentativ Befragten mussten denn auch feststellen, dass Zugangsdaten ausspioniert worden waren.

Das Einfallstor: Infizierte PCs

Per Internet vernetzte PCs sollte man also generell als nicht vertrauenswürdig ansehen. Sie können mit Keyloggern und Sniffern infiziert oder auf manipulierte DNS-Server umgeleitet sein. Das macht sie für eine eindeutige Identifikation ungeeignet. Wer jede Art von Zugängen, seien es Ressourcen im LAN oder VPN-Verbindungen zum Firmennetz absichern will, braucht einen zuverlässigen und eindeutig zuordenbaren zweiten Informationskanal. Die Zwei-Faktor Authentisierung, etwas das man hat und etwas, dass man weiß, macht Identitätsdiebstahl deutlich schwieriger, als beim Einsatz eines einzigen Credentials.

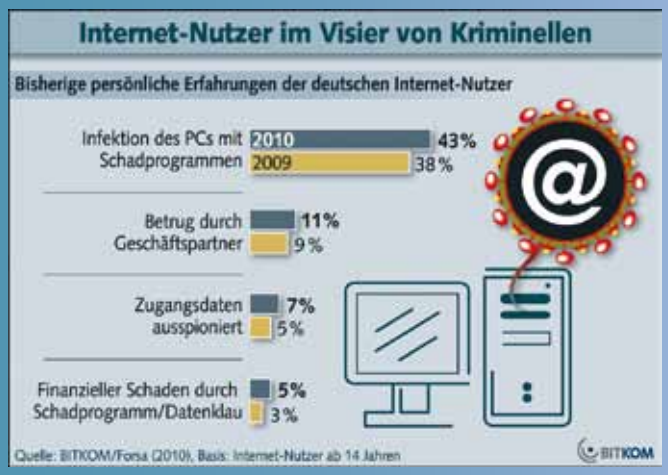
Hier kann sich das Handy mehr und mehr als Sicherheits-Plattform etablieren. Moderne Smartphones sind ja längst weit mehr als nur ein mobiles Telefon: Mit ihnen werden Mails beantwortet, Termine koordiniert oder per GPS Routen geplant und Ziele gefunden. Gegenüber einem normalen Desktop-Computer haben sie aber einen ganz entscheidenden Vorteil: Über die Mobilfunknummer sind sie eindeutig einer Person zuzuordnen. Dieser gesicherte und standardisierte zweite Informationskanal kann Betrügern wirkungsvoll Paroli bieten.

Der zweite Kanal: Smartphones

Dabei bietet schon die einfachste Sicherheitsstufe bei der Mehrfaktor-Authentisierung mit dem Handy ein recht hohes Sicherheitsniveau.

Der Anwender loggt sich dabei wie gewohnt mit seinem Benutzernamen ein, zum Beispiel bei seinem VPN-Remote-Zugang. Danach erhält er vom Authentisierungs-Server eine SMS mit einem Einmal-Passwort zugesandt. Dieses ist nur wenige Sekunden lang gültig und kann nur für einen Login verwendet werden. Ausspionierte Passwörter werden für Hacker nutzlos.

Für eine einfache SMS-Authentisierung muss weder Hard- noch Software verteilt werden. Sie ist für weniger kritische Zugänge durchaus ausreichend und funktioniert mit jedem Mobiltelefon, nutzt aber nicht die Möglichkeiten moderner Smartphones. Diese können ein Einmal-Passwort aus einer Zeitvorgabe oder einem anderen vorgegebenen Parameter selbst errechnen, sodass es nicht mehr im Klartext übertragen werden muss. Aber die leistungsstarke Hardware der Smartphones kann noch mehr: Sie bezieht bei der Berechnung eines Freigabecodes auch Details der jeweiligen Transaktion mit ein. Die so erzeugte digitale Signatur schützt vor Transaktionsverfälschungen, also auch vor dem gefürchteten Man-in-the-Middle-Angriff. Das große Display des Smartphones erlaubt außerdem eine individuelle und übersichtliche GestaltungdesAuthentisierungsdialogs.



Nicht vertrauenswürdig: 43 Prozent aller Internet-Nutzer ab 14 Jahren mussten schon einmal feststellen, dass ihr Rechner mit Viren oder anderen Schadprogrammen infiziert war. Quelle: BITKOM

Die Methode: Mehrfaktor-Authentisierung

Authentisierungs-Systeme wie VASCO Digipass for Mobile gibt es für unterschiedliche Plattformen, zum Beispiel Windows Mobile, Java, Palm oder Blackberry. Der große Vorteil gegenüber anderen Zwei-Faktor Authentisierungslösungen: Es wird keine zusätzliche Hardware benötigt, die konfiguriert und dem Benutzer übergeben werden muss. Der Endanwender bekommt einen Download-Link direkt auf sein Smartphone gesendet. Nach dem Herunterladen des Programms benötigt er nur eine Seriennummer und einen Aktivierungscode, den er per E-Mail oder Telefonanruf erfährt, danach ist das System einsatzbereit. Für die spätere Nutzung des Authentisierungssystems ist immer die Eingabe einer PIN erforderlich. Diese Mehrfaktor-Authentisierung stellt sicher, dass auch im Falle eines Handy-Diebstahls nicht gleich alle Daten-Türen sperrangelweit offenstehen.

Eine sehr interessante Kombination aus Handy und Authentisierungs-Hardware bietet eine neue Generation von Authentisierungssystemen, die direkt auf der SIM-Karte ansetzen, zum Beispiel Digipass Nano. Durch die Miniaturisierung ist es möglich, das komplette Sicherheitssystem auf einem sehr dünnen Film unterzubringen, der auf der SIM-Karte des Handys liegt und mit der Karte zusammen in das Telefon eingeschoben wird. Die auf den Chip untergebrachte Authentisierungs-Software sowie alle Schlüsseldaten sind prinzipiell unangreifbar, sodass dieses System ein sehr hohes Sicherheits-Niveau erreicht. So lässt sich ein Smartphone als vertrautes Endgerät für Authentisierung und digitale Signatur nutzen. Erfahrungsgemäß wird ein Handy weit eher akzeptiert und geht seltener verloren als zusätzlich mitzuführende Hardware-Authentisierungstoken.

Der Einsatz: Bedrohungslage und Anwender

Smartphones werden im Security-Bereich weiter Karriere machen und zu einer ebenso sicheren und integrierten Kommunikation beitragen. Welche Art der Authentisierung die jeweils geeignete ist, hängt von der Bedrohungslage, den zu sichernden Daten und Transaktionen ab, aber auch von der Anwenderstruktur. Sind zum Beispiel ohnehin Firmenhandys im Einsatz, kann diese einheitliche Hardware-Plattform gut für die Authentisierung genutzt werden, da schon eine Deployment-Infrastruktur besteht. Allerdings will sich nicht jeder ein Security-Applet auf sein Handy laden, vor allem dann nicht, wenn es sich um ein privat erworbenes Mobiltelefon handelt. In solchen Fällen ist eine SMS-Authentisierung die bessere Wahl – zumindest, wenn sie keine digitale Signatur benötigt. Sehr hohe Sicherheit und Kompatibilität lässt sich mit Hardware-Zusätzen für die SIM-Karte erreichen.

In vielen Fällen wird die Authentisierungslösung ein heterogenes System sein, dass verschiedene Handymodelle und Sicherheitsstufen bedienen muss. Daher ist es wichtig, dass die unterschiedlichen Authentisierungssysteme in einen einheitlichen Server münden, der die passenden Methoden unter einem Dach vereint. Ebenso wichtig ist eine flexible und verfügbare SDK, das eine individuelle Anpassung an die Kundensituation ermöglicht.

Wer wichtige Zugänge zu seinem Netzwerk wirkungsvoll per Zwei-Faktor Authentisierung sichert, kann auch Angriffe auf digitale Identitäten abwehren, die normalerweise erfolgreich ablaufen. Der gesicherte zweite Informationskanal durch Smartphone oder Handy spielt dabei eine wichtige Rolle. Intelligente Handys werden sich auf absehbare Zeit durchsetzen.