

Mit dem Trend zum mobilen Arbeiten steigen in Unternehmen auch die Anforderungen an den effektiven Schutz sensibler Daten. Gefragt sind Lösungen, die einfach und flexibel auf verschiedenen Geräten einsetzbar sind. Auf Basis der G&D-Technologie bietet Vodafone nun ein standardisiertes, flexibles und vor allem kostengünstiges Produkt für den täglichen Einsatz an.

Im Gegensatz zu den meisten bestehenden Angeboten benötigen Anwender keine separate „Smartcard“ oder sogenannte „Security Token“. Der digitale private Schlüssel und die entsprechenden Zertifikate liegen sicher auf der SIM im Notebook oder Tablet gespeichert. Zusätzliche Hardware – wie Kartenleser etc. – ist nicht erforderlich. Auf der diesjährigen CeBIT in Hannover zeigte Vodafone die Lösung erstmals auf Basis eines Windows 8-basierten Standard Notebooks von Lenovo.

Secure SIM Data verschlüsselt E-Mails und Dokumente so, dass sie für unbefugte Dritte unlesbar sind. Dabei muss der Kunde zum Verschlüsseln und Signieren – ebenso wie für das Entschlüsseln lediglich eine persönliche PIN eingeben. Zum Austausch der E-Mails wird das weitverbreitete Verschlüsselungsprogramm S/MIME genutzt, und zukünftig wird auch eine Verschlüsselung via PGP möglich sein. E-Mails werden auf Wunsch zudem signiert, um Herkunft und unveränderten Inhalt der Mail zu verifizieren.

Zusätzlich zum elektronischen Datenverkehr können auch Speichermedien wie USB-Sticks oder Festplatten mit der Lösung verschlüsselt werden. So bleiben etwa vertrauliche Vertragsunterlagen eines Außendienstmitarbeiters auch bei Diebstahl oder Verlust des Notebooks vor unbefugtem Zugriff geschützt.

eco Report „Internet-Sicherheit 2014“

Ob im Eigenheim oder auf der Autobahn – die Vernetzung und „Smartifizierung“ des Alltags schreiten in großen Schritten voran und war auch 2014 unter den Top-Themen der CeBIT. Die Entwicklung der Technik ist dabei schneller als die Klärung wichtiger Fragen: Denn hinsichtlich zentraler Sicherheitsaspekte im Rahmen der zunehmenden Automatisierung gibt es bundesweit noch deutlichen Nachholbedarf. Zu diesem Ergebnis kommt der aktuelle Report „Internet-Sicherheit 2014“ des eco – Verband der deutschen Internetwirtschaft e. V. (www.eco.de). So gaben rund 93 Prozent der befragten IT-Experten an, dass sich das Sicherheitsbewusstsein für das Thema Smart Home in Deutschland noch sehr stark entwickeln muss. Dr. Bettina Horster, Direktorin Mobile im eco Verband, erklärt: „Die intelligente Haussteuerung bietet unter anderem zahlreiche Schutzmaßnahmen gegen Einbrüche, eröffnet Hackern und Einbrechern aber gleichzeitig neue Angriffsmöglichkeiten – etwa durch elektronische Manipulationen oder Ausspähungen.“

Car2Car: Experten sehen Risiken und Vorteile

Beim Thema Car2Car-Kommunikation waren sich die Experten weniger einig: Rund 24 Prozent sind überzeugt, dass das vernetzte Auto in Zukunft für mehr Sicherheit auf den deutschen Straßen sorgen wird, während rund 36 Prozent glauben, dass die automatisierten Fahrzeuge die Sicherheit sogar senken. Etwa 40 Prozent der Befragten sind der Ansicht, dass sich Vorteile und Gefahren der neuen Technologien aufwiegen. Oliver Dehning, Leiter der Kompetenzgruppe Sicherheit im eco Verband, ist überzeugt: „Die umfassende Car2X-Kommunikation sowie selbstfahrende Autos werden den Verkehr auf deutschen Straßen in wenigen Jahrzehnten grundlegend verändern.“

Entsprechend ist ein völliges Umdenken gefragt: Wie wird mein Fahrzeug vor fatalen elektronischen Attacken geschützt? Wer trägt die Schuld bei einem Unfall? Hersteller, Politik und Justiz müssen in den kommenden Jahren zahlreiche Fragen klären.“

M2M: eco – Verband erwartet umfassende Veränderungen des Alltags

Der wachsende M2M-Trend (Machine-to-Machine) sowie der permanente Datenaustausch zwischen Geräten und Maschinen werden aus Sicht der eco-Experten nicht nur für zahlreiche technische Herausforderungen sorgen.

Der eco Verband erwartet eine umfassende Veränderung des privaten und beruflichen Alltags sowie ein völlig neues Sicherheitsbewusstsein. Vernetzte Häuser und Fahrzeuge spielen bei der Smartifizierung via M2M eine wichtige Vorreiterrolle: Sowie heute bereits Smartphones zu täglichen Begleitern geworden sind, werden Smart Homes und Cars schon in wenigen Jahren kaum noch wegzudenken sein. Umso wichtiger sind laut eco Verband daher eine frühzeitige Klärung zentraler Sicherheitsaspekte, eine Sensibilisierung der Nutzer sowie das Schaffen branchenübergreifender Standards.

Sicheres SINA Tablet auf Surface Pro 2 Basis

Auf der diesjährigen CeBIT haben secunet und Microsoft vorgestellt, wie durch die Kombination aus Sicherheit „Made in Germany“ und einem leistungsstarken Tablet eine vertrauenswürdige, hochsichere und ultramobile Lösung Realität wird. Das gemeinsam vorgestellte SINA Tablet besitzt dieselben Sicherheitsmechanismen, die auch bereits in dem im Hochsicherheitsumfeld bewährten und zugelassenen SINA Workstation Notebook eingesetzt werden.

Die Basis für das SINA Tablet ist das Microsoft Surface Pro 2, das über einen leistungsstarken Intel Core i5 x86 Prozessor verfügt und alle Anwendungen eines PCs auf einem Tablet ermöglicht. Damit ist es eine ideale Plattform für das SINA OS, das in der Virtualisierung das Gastsystem Microsoft Windows 8 einsetzt. Das SINA Tablet bringt die überprüften Funktionen Festplatten-Vollverschlüsselung, Virtualisierung, verschlüsselte Kommunikation (VPN), IP-Telefonie und sichere Authentifizierung von secunet mit und macht das Tablet zu einem Hochsicherheits-Arbeitsplatz.

Microsoft Windows Umgebungen, Microsoft Anwendungen sowie SINA Komponenten gehören zur Standardausstattung in vielen Behörden und Unternehmen und ermöglichen eine leichte Integration des sicheren SINA Tablets. Im täglichen Gebrauch profitieren Administratoren und Anwender dabei gleichermaßen von der einfachen Verwaltung und der Handhabung der Geräte bei einem für diese Geräteklasse bis jetzt noch nicht erreichten Sicherheitsniveau.

Durch den Einsatz von Microsoft Windows 8, im von SINA vertrauenswürdig geschützten Gastsystem, bleibt die vollständige Applikationswelt erhalten; durch die flexiblen Einsatzmöglichkeiten des Microsoft Surface 2 als Desktop, Notebook und Tablet benötigt der Anwender nur noch ein Gerät.

Alle Daten sind immer geschützt und der Nutzer erhält eine identische Sicht auf Arbeitsplatz und Anwendungen. Darüber hinaus entfällt eine fehleranfällige Synchronisation von Daten und Dokumenten zwischen unterschiedlichen Geräteklassen.

Das SINA Tablet wird neben dem SINA Workstation Notebook das zweite hochsichere Gerät von secunet sein, das die Kundenbedürfnisse an Mobilität und hoher Sicherheit erfüllt. Es bietet, ge-