SySS GmbH
Sebastian Schreiber
Senior IT Security Consultant
Wohlboldstraße 8
72072 Tübingen

Safer Computing

Sehr geehrter Herr Schreiber,

kürzlich lieferte ein Spediteur eine schwere Palette bei mir im Büro an. Sie war so schwer, weil sich darauf ein Safe befand. Den habe ich mir bestellt, nachdem ich Ihrer Demonstration auf der Pressekonferenz im Vorfeld der IT & Business und DMS EXPO beiwohnte. In sehr kurzer Zeit haben Sie dort das Betriebssystem eines Tablet Computers ausgetauscht und danach auch den Zahlen-Code als Passwortschutz für den Zugang zu den auf dem Tablet befindlichen Dateien geknackt (nächste Demo auf der IT & Business/DMS EXPO an allen drei Messetagen jeweils um 17 Uhr im Forum in Halle 3). Da war für mich klar: eine Software- oder Hardware-gestützte Verriegelung alleine schützt meine Daten nicht vor fremdem Zugriff. Nun möchte ich zwar nicht, dass meine privaten Dateien oder Firmendaten in fremde Hände gelangen, aber das Interesse daran dürfte wohl doch eher gering sein.

Ganz anders sieht die Sache aber bei Unternehmen aus, deren wirtschaftlicher Erfolg auf der Geheimhaltung ihres Know-hows basiert. Man denke dabei nur mal an die Rezeptur von Coca Cola.

IT-Administratoren könnten nun ihren Mitarbeitern untersagen, diese Daten außer Haus mitzunehmen beziehungsweise von außerhalb darauf zuzugreifen. Aber dadurch gingen Produktivitätsvorteile verloren und Umsatzmöglichkeiten würden nicht realisiert. Zudem dezentralisiert sich die Arbeit immer mehr und globale Teams brauchen Software-gestützte Kommunikations- und Collaboration-Lösungen um von verschiedenen Orten aus interagieren zu können. Viele Mitarbeiter möchten auch ihr mobiles Endgerät selbst auswählen (Bring your own Device), mit dem sie von jedem Ort aus arbeiten können.

Safes in Hotelzimmern schützen darin befindliche Rechner vor unerlaubtem Zugriff. Aber im parkenden Firmenwagen oder auf einer Konferenz besteht dieser Schutz nicht. Und in Taxen oder am Flughafen sind schon viele Smartphones verloren gegangen. Wie aber können Unternehmen dann ihre Daten wirksam vor unerlaubten Zugriff schützen?

Gespannt warte ich auf Ihre Antwort
Mit freundlichen Grüßen

Eberhard Heins,
Chefredakteur *is report*

Antwort Seite 54

Komplexität bildet das Hauptproblem

Moderne Verschlüsselung ist nicht zu brechen. Die Schwierigkeit besteht darin, die Systeme wirksam zu betreiben. Selbst winzige Fehler können dazu führen, dass ein ansonsten hochsicheres System mühelos aufzubrechen ist.

GRATULATION zum neuen Tresor, sehr geehrter Herr Heins! Verglichen mit IT-Security-Produkten hat er enorme Vorteile: er verlangt kaum Pflege, Fehlbedienungen sind unwahrscheinlich, Sie können ihn auch in zehn Jahren noch nutzen – und selbst versierte Viren und Würmer finden keinen Einlass. Aus diesem Grund habe ich für SySS sechs dezentrale Tresore beschafft.

Nicht immer aber ist man zuhause und genießt den selbst installierten Sicherheitsstandard. An öffentlichen Orten wie Flughäfen, Bahnhöfen oder auch in Taxen können Geräte leicht verloren oder entwendet werden. Im Hotel angekommen, wähnt man sich durch den hoteleigenen Safe in Sicherheit. Aber vertrauen Sie den Tresoren in Hotels wirklich? Das Magazin *Wired* zeigt, wie ein Kind von vielleicht fünf Jahren vergnügt glucksend unterschiedliche Waffentresore knackt – mit einfachen Werkzeugen: mit Büroklammern und einem Strohhalm.

Sicherheitssysteme sind oftmals nur scheinbar sicher und lassen sich schon mit wenig Mühe überwinden, das gilt für virtuelle Sicherheitssysteme leider ebenso wie für solche mit physischer Präsenz. Einen standardmäßig mit Bitlocker verschlüsselten Laptop knacken wir in Sekunden. Doch Daten können nur dann nutzen, wenn sie auch reisen. Die Lösung, Daten nicht aus dem Haus zu geben, funktioniert nicht – schließlich müssen wir in unserem Fall sensible Projektberichte an Kunden übergeben; und meine Mitarbeiter reisen über den gesamten Globus um Projekte durchzuführen.

Daten werden immer häufiger gestohlen: man denke an die sogenannten Steuer-CDs aus Liechtenstein und der Schweiz. Daten und Informationen haben sich zu bedeutenden Wirtschaftsfaktoren und zu einer begehrten Ware entwickelt. Die wachsende Abhängigkeit in Verbindung mit Begehrlichkeiten auf wertvolle Daten hat auch zu einer Steigerung der Leistungsfähigkeit von Angriffstools geführt: während früher Sicherheitsaktivisten kleine, mehr schlecht als recht arbeitende Exploits geschrieben haben, um die Existenz von Schwachstellen nachzuweisen, werden heute von Unternehmen leistungsstarke Angriffswerkzeuge hergestellt, die abgestimmte Angriffe auf verschiedenen Ebenen durchführen. Moderne Angriffswerkzeuge, wie Botnetze oder Stuxnet, sind wirkungsmächtig und dienen Nutzern aus dem Bereich der organisierten Kriminalität oder auch staatlich motivierten Tätern. Viele Angriffswerkzeuge sind käuflich – bezahlt wird per Kreditkarte.

Ihre Frage nach dem Schutz von Daten verlangt also geradezu nach der Antwort: „Verschlüsseln Sie Ihre Daten doch einfach!“ Mit modernen – oft kostenlos verfügbaren – Tools lassen sich Daten sowohl auf Massenspeichern als auch auf dem Transport derart wirksam verschlüsseln, dass Angriffe ausgeschlossen werden können. Moderne Verschlüsselung ist also quasi nicht zu brechen.

Die Schwierigkeit besteht darin, die Systeme wirksam zu betreiben: selbst winzige Fehler können dazu führen, dass ein ansonsten hochsicheres System mühelos aufzubrechen ist. Oftmals haben Softwareprodukte Fehler, sind schlecht gepflegt oder falsch konfiguriert. Oft geben Unternehmen vertrauliche Daten an Dienstleister aller Art weiter oder beauftragen Subunternehmer, die dann ebenfalls Subunternehmer beauftragen.

Komplexität ist immer die Hauptursache von Fehlern gewesen. Ein aktuelles Beispiel bietet sich uns beim Bau des Berliner Großflughafens sogar mit sichtbaren Konsequenzen: eine erhebliche Verzögerung und exorbitante Mehrkosten. Die Beauftragung von Sub-Sub-Unternehmen führte darüber hinaus dazu, dass ausgerechnet ein polizeibekannter Islamist auf der Baustelle im Sicherheitsbereich als Mitarbeiter eingesetzt wurde.

Bei der Erstellung und dem Betrieb von IT-Lösungen ist die Komplexität ebenfalls das Hauptproblem – während man funktionale Mängel identifiziert und diese behoben werden, bleiben sicherheitsrelevante Defizite in aller Regel von den IT-Experten unidentifiziert und werden daher auch nicht behoben.

Die letzte Bastion der Absicherung der Systeme muss der Penetrationstest sein: erfahrene Experten im „Hacking“ identifizieren Schwachstellen durch die Simulation aktiver Attacken. Denn nur wenn man die Lücken kennt, kann man sie schließen.

Der Absender

Sebastian Schreiber ist Managing Director, Senior IT Security Consultant bei der SySS GmbH.