atsec the information security provider
NEWS 02/11

Erbsenzählen als Sicherheitskonzept

Die Sicherheitsbranche hat ein neues Allheilmittel entdeckt – Checklisten. Gaukelt doch dieser Begriff eine Sicherheit vor, die bei genauerem Hinsehen schlicht das Gegenteil bedeutet. Eine Checkliste ist schnell erstellt, dafür entwickelt, abgehakt zu werden und sich über die aufgeführten Punkte möglichst wenig – oder gar keine – Gedanken zu machen. Da richtige Sicherheitsaudits aufwendig sind, suchen viele ihr Heil in solchen Listen, die ein trügerisches Gefühl von Objektivität und Messbarkeit erzeugen, welches man bei den individuellen und bohrenden Fragen der Auditoren oft vermisst.

Leider beginnen solche Checklisten sehr schnell, ein Eigenleben zu führen und sich von ihrem ursprünglichen Zweck zu entkoppeln. An Beispielen mangelt es da nicht: Kürzlich wurde ich in der Sicherheitskontrolle eines Flughafens festgehalten, weil im Handgepäck meine Zahnpasta in einem nicht normgerechten Plastikbeutel steckte. Ein paar Monate zuvor scheiterte ich an einer Supermarktkasse in den USA mit dem Anliegen, ein Bier einzukaufen. Nun feierte ich schon vor einiger Zeit meinen 50. Geburtstag, die Angestellten dort waren aber nicht in der Lage, festzustellen, dass ich über 21 bin. Bei der zwingend erforderlichen Prüfung meines Alters auf meinem Personalausweis verstanden sie es nicht, das Geburtsdatum zu entziffern – war es doch ungewöhnlicherweise nicht in amerikanischer Notation vermerkt. Ersatzweise die Person anzusehen und mit gesundem Menschenverstand festzustellen, dass der Typ da seine Jugend wohl eine Weile hinter sich hat, stand nicht auf der Checkliste.

Vor Kurzem wollten nun Auditoren in unserer Prüfstelle durchsetzen, dass wir alle Besucher mit einem Besucherausweis versehen. Was in großen Unternehmen sicherlich sinnvoll ist, wirkt in unserem kleinen Büro nur lächerlich, weil natürlich jeder jeden kennt und ein Besucher – mit oder ohne Ausweis – nie als Mitarbeiter durchgehen würde.

> *„Forget a perfect checklist... A key skill is: knowing when to ignore it!“*

Nach und nach machen sich Checklisten nun auch in den Köpfen derer breit, die über die Zukunft von Sicherheitsstandards wie der Common Criteria nachdenken. Das macht mir wirklich Angst. Auch wenn die Motive durchaus ehrenhaft sein mögen: meine Erfahrung ist, dass mit der Zeit Verstehen durch Erbsenzählerei ersetzt wird. Das erzeugt kein Vertrauen, und damit schafft sich der Standard auf lange Sicht ab.

Freilich, auch ich verwende Checklisten. Bei Prüfungen soll ja kein wichtiger Aspekt vergessen werden. Matt Bishop hat es aber in einem seiner Vorträge zum Thema[1] auf den Punkt gebracht: Das wichtigste an einer Checkliste ist, zu wissen, wann man sie ignorieren muss! Eine Checkliste ist ein Hilfsmittel und kein Selbstzweck. Das Ziel bleibt Sicherheit. Und das wird bei atsec auch so bleiben!

Herzlichst,

Gerald Krummeck
Prüfstellenleiter atsec

1 *http://www.cio.ca.gov/OIS/Government/events/documents/ca3.pdf*

BSI-Kongress in Bonn

„Sicher in die digitale Welt von morgen“ – unter diesem Motto findet am 10. - 12. Mai 2011 der 12. Deutsche IT-Sicherheitskongress in Bonn statt. Eine Begleitausstellung, 42 Vorträge, vier Keynotes und eine hochrangig besetzte Podiumsdiskussion zum Thema Cloud Computing informieren die Teilnehmer über neueste Entwicklungen, Gefahren und Chancen der Informationstechnik und laden zum fachlichen Diskurs ein. Weitere Themen sind z.B. Cyber Sicherheit, sichere Plattformen, ISMS, Entwicklungen in der Kryptographie sowie der neue Personalausweis. atsec präsentiert sich auf einem attraktiven Standplatz (F8) und freut sich auf Ihren Besuch.

atsec hilft in der Not

Soziales Engagement und das Bewusstsein für ökologische Verantwortung wird bei atsec seit jeher großgeschrieben. Im Angesicht des verheerenden Erdbebens in Japan entschloss sich atsec mit allen Mitarbeitern zu einer vierstelligen Spende an das Rote Kreuz, um einen kleinen Beitrag zur Linderung der Not zu leisten.

atsec it security blog
Verfolgen Sie brandaktuell Diskussionen und Erlebnisse unserer Mitarbeiter auf http://atsec-information-security.blogspot.com

Smartphones – bedingt abwehrbereit

Smartphones sind mobile Kommunikationszentrale, dienen als Terminkalender und speichern große Mengen an persönlichen und geschäftlichen Daten. Neben dem Risiko, dass durch Verlust oder Diebstahl Daten abhanden kommen, bergen Smartphones durch ihre konstante Online-Verbindung weitere Gefahren in sich. Die Installation optionaler Komponenten (Apps) vergrößert die Angriffsfläche zusätzlich.

Risiken

Abhängig von der Nutzung der Smartphones ergeben sich folgende Risiken:

Sensitive Daten auf dem Telefon

Auf Smartphones werden zunehmend sensible Daten gespeichert, von personenbezogenen Informationen (Adressbuch) über gespeicherte E-Mails und Passwörter, Instant-Messenger-Protokolle und Notizen bis hin zu geschäftlich relevanten Dokumenten. Im Kalender stehen nicht nur Termine selbst, sondern auch Geschäftspartner, Rufnummern und PINs für Telefonkonferenzen und weitere Notizen.

Telefonmissbrauch

Da Smartphones meist dauerhaft online sind, gewinnen sie auch für Botnetz-Betreiber an Bedeutung. Genau wie übernommene PCs lassen sich Smartphones aktiv als Werkzeug für das Versenden von SPAM als Email, SMS oder auch DDOS-Angriffe missbrauchen. Der unbemerkte Aufbau von Verbindungen zu teuren Servicenummern durch Schad-Applikationen ist ein lukratives „Geschäftsfeld".

Privatsphäre

Neben den Daten auf dem Telefon ist auch der Ort, an dem sich das Telefon bzw. sein Besitzer befindet, interessant. So lassen sich Bewegungsprofile erzeugen und das Kommunikationsverhalten, beispielsweise der Zeitpunkt der Kontaktaufnahme und die Identität der Kommunikationspartner, auswerten. Lediglich bei Social Networking Applikationen (Facebook, Twitter, Google Latitude,...) stellen manche Benutzer diese Informationen freiwillig zur Verfügung – eine darüber hinausgehende Auswertung oder Weitergabe ist selten in seinem Interesse.

Freund oder Feind?

Die Gegenspieler lassen sich in vier Gruppen einteilen:

Marketing

Gezielte Werbung ist ein mächtiger Markt. Je genauer Zielgruppen angesprochen werden, desto größer der Erfolg – so wird standortbezogene Werbung immer attraktiver. Anhand von Bewegungsprofilen und der Suche nach Schlagwörtern im Speicher des Smartphones wird Werbung äußerst zielgerichtet platziert. Das Adressbuch liefert weitere Empfänger für gezielte Werbeaktionen.

(Wirtschafts-) Spionage

Sensitive Daten, die auf Smartphones gespeichert werden, sind für Wirtschaftsspione ein lohnendes Ziel. Termine im Kalender ebenso wie Adressbucheinträge geben Aufschluss über Kundenbeziehungen. Relevante E-Mails und erhebliche Speicherkapazitäten beinhalten oft vertrauliche Informationen.
Zudem lässt sich das Telefon über spezielle Apps als ferngesteuerte „Wanze" einsetzen und der Telefon- und Datenverkehr mitschneiden.

Cyberkriminelle

Vom Versenden kostenpflichtiger SMS bis hin zum Missbrauch des Smartphones in Botnetzen gibt es vielfältige Methoden, die von Kriminellen direkt ausgenutzt werden. Auch der Verkauf gesammelter Adressdaten von Mobiltelefonen gehört zu den illegalen Aktivitäten der Szene.

Nachrichtendienste

Es gibt in einigen Staaten Dienste, die ein deutlich über die reguläre Strafverfolgung hinausgehendes Interesse daran haben, Informationen über den Aufenthaltsort von Personen, deren Art und Weise der Kommunikation zu bestimmten Zeitpunkten und deren Kontaktpersonen zu erhalten. Diese Informationen werden zum Teil auch über Mobilfunkbetreiber erfasst, sind aber wesentlich detaillierter, wenn sie direkt von einem Smartphone mit GPS-Empfänger gelesen werden.

App Markets

Schwierig gestaltet sich die Unterscheidung zwischen vertrauenswürdigen und schädlichen Apps. Für die meisten Plattformen gibt es offizielle und inoffizielle Quellen für Apps, die sogenannten Markets. Bei den von den Plattform-Herstellern bereitgestellten Markets wird eine gewisse Kontrolle über die Inhalte ausgeübt, die Fremd-Quellen bieten eine solche Sicherheit nicht. Eine große Anzahl von Trojanern etwa findet sich in inoffiziellen chinesischen Markets. Aber auch in den von Herstellern kontrollierten Märkten werden immer wieder Applikationen ermittelt, welche die Privatsphäre verletzen. Einerseits dürfte sich der Aufwand für die Prüfung der Vielzahl von Applikationen in Grenzen halten, andererseits werden Verstöße von manchen Herstellern wohl in Kauf genommen. Die vom Hersteller offiziell sanktionierten Märkte bieten somit keine Garantie für sichere Software.

Werbefinanzierte Apps sind mittlerweile lukrativer als Apps, für die eine Lizenzgebühr fällig wird. Solche Werbe-Einblendungen werden durch Bibliotheken realisiert, welche die App-Programmierer von Dritten beziehen. Einige dieser Bibliotheken sind bzgl. des Datenschutzes bedenklich, greifen sie doch auf Positionsdaten zu, durchforsten persönliche und sensitive Daten auf den Smartphones und leiten diese nicht selten auch weiter.

Gegenwehr

Abhängig von der Plattform gibt es prinzipiell zwei Mechanismen, die Rechte von Applikationen und somit deren Informationshunger zu kontrollieren. Zum einen geschieht dies durch Vorgaben des Herstellers für die Zulassung zum Markt, die dann gemeinhin durchgesetzt werden, etwa beim iPhone. Bei Android-basierten Systemen gesteht der Benutzer bei der Installation der App bestimmte Rechte zu – oder verzichtet auf die App. Allerdings garantiert keine dieser Vorgehensweisen Sicherheit oder verhindert Missbrauch.
Eine werbefinanzierte App erfordert beispielsweise Internetzugriff. Für den Benutzer ist jedoch nicht erkennbar, ob damit tatsächlich nur Werbung geladen oder aber auch Informationen durch die App nach außen weitergegeben werden.

Fremdbestimmt

Unabhängig von der persönlichen Rechtevergabe und Kontrolle über installierte Apps gibt es bei allen Smartphone-Systemen die Option, Apps seitens der Hersteller – unabhängig von einer Benutzerzustimmung – zu installieren oder zu löschen. Letztendlich kontrolliert nicht der Anwender seinen mobilen Kleinrechner, sondern Hersteller und Netzbetreiber.

Sicherheitsmodell

iPhones wie Androiden verwenden UNIX-basierende Betriebssysteme – somit stehen hier Sicherheitsmechanismen von UNIX zur Verfügung.
Das iOS von Apple führt Applikationen in einer separaten Sandbox aus, welche die verfügbaren Betriebssystem-Dienste einschränkt. In der Sandbox sind die erlaubten System-Calls eingeschränkt und Restriktionen bezüglich der sichtbaren Dateien, Netzwerkressourcen, Hardware und Konfigurationsdaten gesetzt. Weiterhin wird ein Verschlüsselungsmechanismus für Benutzerdaten angeboten.
Android verwendet einen ähnlichen Mechanismus: Apps werden hier in voneinander getrennten Bereichen ausgeführt, die erst nach Freigabe durch den Benutzer untereinander kommunizieren dürfen. Die Trennung erfolgt bei der Installation und Ausführung von Apps, mit einer für jede App dedizierten Benutzer-ID auf dem System. Da auf wechselbare SD-Karten alle Applikationen gleichermaßen Zugriff haben, greift dieser Trennmechanismus nur für Daten auf dem internen Speicher.
Die Sandbox-Systeme verhindern theoretisch den Zugriff bösartiger Apps auf die Daten anderer Apps. In der Praxis werden diese Verstöße allerdings hinter einem legitimen und vom Benutzer autorisierten Zugriffsrecht versteckt.

No Risk, No Fun?

Bei Beachtung einiger grundlegender Sicherheitsmaßnahmen lassen sich Smartphones mit minimierten Risiken nutzen. Entscheidend ist die Beschränkung auf die tatsächlich notwendigen Apps. Diese sollten nur von offiziellen Quellen, also Markets der Plattform-Hersteller, bzw. von als sicher eingestuften Seiten geladen werden – ähnlich wie auch für PCs. Von werbefinanzierten Apps ist generell abzusehen, da aufgrund der eingebundenen Fremdbibliotheken das Risiko hoch ist, dass sensitive Daten an Dritte übertragen werden. Eine völlige Garantie gegen bösartige Apps ist so zwar nicht gegeben, die Wahrscheinlichkeit, sich Schadsoftware einzufangen, wird allerdings erheblich reduziert.
Bei Plattformen, die die Vergabe von Berechtigungen bei der Installation anfordern, ist unbedingt zu prüfen, ob die App für ihre eigentliche Funktion tatsächlich alle geforderten Rechte benötigt. Ein Email-Programm, das Informationen über die aktuelle Position verlangt, ist genauso verdächtig wie ein Bildschirmschoner, der eine SMS lesen möchte. Internetzugriff ist in der Kombination mit Rechten für Datenspeicher und persönliche Daten nur für sehr wenige Applikationen notwendig. Die Nachverfolgung aktueller Sicherheitswarnungen zur eingesetzten Plattform ist eine weitere unerlässliche Grundlage für die effektive Absicherung.
Einen Sonderfall stellen Smartphones mit Jailbreak („rooted“) dar. Hier lassen sich zusätzliche Sicherheitsmechanismen, wie etwa Firewalls, die Verbindungen zu Adware-Servern unterbinden, Speicherverschlüsselung oder Krypto-Telefonie, installieren. Allerdings erlangen so auch schädliche Apps umfassende Kontrolle über das Smartphone – unabdingbar ist also die Restriktion auf wenige vertrauenswürdige Apps.

Die Zukunft ...

Unabhängig vom Hersteller oder Betriebssystem des Smartphones wird Software immer ein gewisses Risiko für die Privatsphäre und die Vertraulichkeit von Informationen darstellen – das ist bei PCs seit vielen Jahren nicht anders.
Für sensitive Bereiche wäre eine unabhängige Zertifizierungsstelle wünschenswert, die Betriebssysteme und Apps bzgl. Datenschutz und Sicherheitskriterien prüft und zertifiziert. Realistisch ist dies allerdings aufgrund des hohen Prüfaufwandes (Quellcode-Analyse, etc.) nur für kommerzielle Apps mit hoher Verbreitung.
Der beste Schutz bleibt die Einsicht, nur wenige, vertrauenswürdige Apps zu verwenden – in Unternehmen geben konkrete Richtlinien die Kriterien hierfür vor.
Solange die Smartphones kein flexibleres Rechtekonzept implementieren, spielt die organisatorische Sicherheit eine zentrale Rolle – die Benutzer sind letztlich der Schlüssel für den verantwortungsvollen Umgang mit Technik und Informationen.

Referenzen

http://blogs.wsj.com/wtk-mobile/
http://www.heise.de/meldung/IPv6-Smartphones-gefaehrden-Privatsphaere-1168416.html

atsec NEWS

atsec und ISCCC

Am 14. März 2011 besuchte eine Delegation des ISCCC (China Information Security Certification Center) unter der Leitung ihres Direktors, Herrn Wei Hao, die atsec-Zentrale in München.

Bei der offenen und freundlichen Begegnung stellten die beiderseits gut vorbereiteten Parteien ihre Tätigkeiten im Bereich der Produktevaluierung und -zertifizierung vor, tauschten diesbezügliche Erfahrungen aus und diskutierten Themen der Informationssicherheit. In einem Ausblick legte atsec zudem die Chancen dar, die sich durch eine Teilnahme Chinas am Common Criteria Recognition Arrangement (CCRA) für den chinesischen Markt ergeben könnten.
Herr Wei Hao kommentierte dieses Treffen: „Wir freuen uns über diesen weiteren Besuch bei atsec, die als Prüfstelle für Informationssicherheit in Deutschland, USA und Schweden akkreditiert ist und somit weltweit viel Erfahrung in der Evaluierung auf diesem Gebiet vorweisen kann. Ich glaube, dass die Zusammenarbeit mit atsec in China für die chinesische Industrie und internationale Hersteller im Bereich Informationssicherheit sehr vorteilhaft wäre."
Staffan Persson, Geschäftsführer von atsec Deutschland, erklärte: „Es ist uns eine Freude, das ISCCC in unserer Geschäftsstelle in München zu begrüßen. ISCCC ist die Behörde für Informationssicherheit in China. atsec ist ein internationales Unternehmen; viel bedeutsamer ist allerdings, dass wir unsere Leistungen mit den örtlich relevanten Akkreditierungen im jeweils entsprechenden Land anbieten. Wir verfügen über höchste Integrität und sind uns des Interesses unserer Kunden bewusst, Informationssicherheit unabhängig und ohne Einfluss von außen zu verbessern. Wir freuen uns auf weitere geschäftliche Gespräche und eine Zusammenarbeit mit ISCCC in China."
Nach dem Besuch bei atsec Deutschland traf sich die chinesische Delegation mit deutschen und schwedischen Vertretern des CCRA und des Common Criteria Development Boards (CCDB), um sich über das internationale Verfahren zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten sowie über die aktuellen Weiterentwicklungen der Common Criteria zu informieren.

Über das China Information Security Certification Center

Das China Information Security Certification Center (ISCCC) ist von der staatlichen Behörde für Reformen im öffentlichen Sektor anerkannt und von acht Verwaltungen, wie der Informationsagentur des chinesischen Kabinetts und der Zertifizierungs- und Akkreditierungsverwaltung der Volksrepublik China autorisiert. ISCCC ist die einzige Stelle, die für die Zertifizierung von Informationssicherheit in Übereinstimmung mit den Vorschriften der Zertifizierungs- und Akkreditierungsverwaltung der Volksrepublik China und Anwendungsbestimmungen, einschlägigen nationalen Gesetzen und Richtlinien der obligatorischen Zertifizierungen und der Verwaltung der Informationssicherheit zuständig ist.

SupplyOn bietet Plattform für unternehmensübergreifende Zusammenarbeit

Die SupplyOn AG ist weltweit führender Anbieter einer webbasierten Plattform für die unternehmensübergreifende Zusammenarbeit in der Fertigungsindustrie. Im Fokus stehen dabei die Branchen Automobil- sowie Luft- und Raumfahrtindustrie. Über die Plattform werden Prozesse in den Bereichen Einkauf, Logistik, Qualitätsmanagement und Finanzen abgewickelt. SupplyOn zählt namhafte Unternehmen wie Airbus / EADS, BMW Group und Bosch zu seinen Kunden.
In der Automobil- und Fertigungsbranche und in noch größerem Umfang in der Luftfahrt hat die Einhaltung von IT-Sicherheitsrichtlinien hohe Priorität. atsec unterstützte die SupplyOn AG bei der Erstellung der Sicherheitskonzepte für ihre Plattform. Im Speziellen wurden die Kommunikationswege zwischen Herstellern, Zulieferern und SupplyOn analysiert und Maßnahmen zum Schutz sensitiver Informationen erarbeitet. So wird sichergestellt, dass nur berechtigte Partner Daten austauschen und diese Daten vor unbefugten Dritten geschützt sind.

IMPRESSUM

atsec information security GmbH
Steinstr. 70
81667 München
Deutschland
Telefon: +49-89-442-49-830
Telefax: +49-89-442-49-831
E-Mail: info@atsec.com

Vertretungsberechtigte Geschäftsführer:
Salvatore la Pietra
Staffan Persson

Registernummer: HRB 129439
Registergericht: Amtsgericht München
UST-ID-Nr. gemäß § 27a UStG:
DE205370914

Verantwortlich für den Inhalt:
Peter Wimmer (Anschrift s.o.)