



ix extra

Security

Malware-Trends

Malware-Trends bei Jägern und Gejagten

Komplexer Schutz gefragt Seite I

Neue Gefahren im Web 2.0

Kriminelle Dienstleistung Seite V

Smartphones im Visier der Cyberkriminellen

Malware mit Ansage Seite X

Vorschau

Embedded Systems
Industrietaugliche I/O-Komponenten Seite XII

Veranstaltungen

20. – 21. September 2011, Oldenburg

DACH Security
www.syssec.at/dachsecurity2011

20. – 22. September 2011, Stuttgart

IT & Business
www.messe-stuttgart.de/cms/business11_blick0000.0.html

18. – 20. Oktober 2011, Kopenhagen

VMWorld Europe 2011
www.vmworld.com

22. – 23./28. – 29. November 2011, München/Hannover

Kerberos – Single Sign-On im gemischten Linux- und Windows-Umfeld
www.ix-konferenz.de

28. September 2011, Köln

Hyper-V sicher und sauber

ix extra
Security zum Nachschlagen:
www.heise.de/ix/extra/security.shtml

sponsored by:



McAfee



Essential Security
against Evolving Threats™

Security

Komplexer Schutz gefragt

Malware-Trends bei Jägern und Gejagten

Die Bedrohungslage durch Malware nimmt stetig an Komplexität zu. Schutz kann nur eine Kombination aus Technik und Methodik bieten, die auch den Faktor Mensch einbezieht.

Moderne Schadsoftware und die treibenden Kräfte dahinter zeichnen sich durch eine zunehmende Professionalisierung aus. Während sich typische Auswirkungen noch vor 10 bis 15 Jahren als grafisch ansprechende Spielereien oder destruktives Löschen mit Proof-of-Concept-Charakter zeigten, prägen heute ausgeklügelte kriminelle Geschäftsmodelle das Bild. Die Vermietung von Bot-Netzen für massenhaften Spamversand oder DDoS-Angriffe, Vorgaukeln von Infektionen zum Verkauf von Pseudo-Schutzprodukten (Scareware) und trojanische Pferde zum Abfangen und Umleiten verschlüsselter Finanztransaktionen sind nur einige bekannte Beispiele.

Komplexe Gefährdungen

In dem fortwährenden Hase- und-Igel-Spiel zwischen Angreifern und Herstellern können Letztere bereits heute nur schwer mithalten. Web 2.0, Smartphones, Cloud Computing – angesichts der aktuellen Trends zeichnen sich völlig neue Herausforderungen für die IT-Sicherheit ab. Individuelle,

zuvor unbekannte Gefährdungen werden nur sporadisch bekannt und erscheinen oftmals wie aus dem Nichts.

Eines der neuen Problemfelder bildet das Web 2.0 mit seinen komplexen, global aktiven Social Networks. Neben technischen Lücken, etwa beginnend mit Cross-Site Scripting, die in der Vergangenheit beispielsweise eine massenhafte Verbreitung von Schadsoftware und Falschmeldungen, das Ändern von Kennwörtern fremder Accounts oder das Mitlesen fremder Chats ermöglichten, geht es um Datenschutzprobleme. Im Fall Facebook zeigte dies etwa der kürzlich publik gewordene Fall der Geburtstags-einladung von „Thessa“, die ungewollt ein großes öffentliches Echo auf sich zog, aber auch die Einführung der automatisierten Gesichtserkennung bei hochgeladenen Fotos. Auch die – aus datenschutzrechtlicher Sicht offenbar bewusst lose gewählten – Standardeinstellungen der Betreiber mahnen einen sensiblen Umgang mit diesen neuen Medien an.

Auch beim Cloud Computing geraten Datenschutzaspekte in den Blick. Vieles ist noch ungeklärt, etwa wem man die Daten

eigentlich anvertraut und welche Kontrolle darüber besteht. Mit einer Schwachstelle in der SOAP-Schnittstelle der quelloffenen Cloud-Computing-Infrastruktur Eucalyptus haben Experten bereits eine Sicherheitslücke nachgewiesen, bei der Angreifer über die Wiederverwendung mitgelesener Signaturen beliebige Befehle im Namen anderer Nutzer in der Cloud ausführen konnten. Darüber, ob und welche zukünftigen Gefahren von potenziell auf die Cloud zugeschnittener Schadsoftware ausgehen, lässt sich derzeit allenfalls spekulieren. Beispielsweise darüber, ob die Betreiber von Bot-Netz-Verbänden in Zukunft auch Cloud-Infrastrukturen, die von vielen Opfern genutzt werden, zum Aufbau einer neuen Generation von Angriffswerkzeugen missbrauchen könnten.

Einfallstor Smartphone

Auch mobile Endgeräte wie die allseits beliebten Smartphones zeichnen sich zurzeit durch immer mehr öffentliche Sicherheitslücken aus. Zuletzt belegte dies nicht nur der iPhone-Geodatenskandal. Auch eine gleich in mehreren Android-Apps gefundene Lücke unterstreicht diesen Trend: Von den Google-Servern vertraulich erhaltene Authentifizierungs-Token wurden unverschlüsselt weitergereicht und ließen sich so von mitlesenden Angreifern für Identitätsübernahmen einsetzen. Die Zahl der Schadsoftware für Smartphones, die unter anderem in regulären Apps auftaucht, steigt überdurchschnittlich stark an. So erwartet beispielsweise Kaspersky für 2011 eine Verdopplung der Virensignaturen für mobile Endgeräte.

Zählte man 2005 noch 1,7 Millionen verschiedene Schadprogramme, so war man Ende 2010 bei über 55 Millionen angelangt. Beide Entwicklungen haben sich in letzter Zeit etwas

verlangsamt und das Wachstum flacht ab. Dies liegt allerdings nicht am Aussterben von Schadsoftware, sondern zum einen an wesentlich diversifizierteren Verbreitungswegen wie über Smartphones oder soziale Netzwerke und an der Abkehr von dateibasierenden Angriffen. So ist beispielsweise bei direkten Angriffen auf die Dienste-Server kein Einschleusen von Schadprogrammen auf die Endbenutzersysteme nötig, sodass diese Angriffe nicht mehr in die klassischen Statistiken fallen. Zum anderen haben sich die Reaktionsmöglichkeiten der Sicherheitssoftware stark ausgeweitet, sodass Signaturrekennung nur noch einen kleinen Teil der Fähigkeiten abdeckt und immer mehr Schadsoftware mit anderen Verfahren, wie verhaltensbasierenden Heuristiken oder Reputationsabfragen, zu erkennen sind. Auch die organisierte Kriminalität hat diese modernen IT-Infrastrukturen längst für sich entdeckt. So tauchten bereits trojanische Pferde auf, die auf Mobiltelefonen Transaktionsnummern des mTAN-Verfahrens abfangen, das über den vermeintlich sicheren Weg SMS die im PC-Bereich verbreitete Banking-Malware zu meiden sucht.

Zudem eröffnen die bei Smartphones und Spielekonsolen beliebten Jailbreaks (die das Installieren und Ausführen beliebiger, vom Systemhersteller nicht freigegebener Software erlauben) neue Angriffsmöglichkeiten, die obendrein in der Regel völlig freiwillig durch die Benutzer selbst auf die Geräte gelangen. Es ist keineswegs nur eine Schutzbehauptung der Hersteller, unautorisierte Veränderungen am Betriebssystem als Hauptursache für Instabilität, Dienststörungen und andere Probleme anzuprangern. Erst kürzlich zeigten koreanische Forscher, dass sich den Nutzern derartiger Software unbemerkt Schadcode unterschieben lässt

– und in der Folge Spielekonsole oder Smartphone zu einer möglicherweise längerfristig unerkannten Angriffsquelle im eigenen LAN mutieren.

Wie eine Reihe akademischer Nachweise der letzten Zeit zeigen, könnte zukünftig sogar die in modernen Automobilen verbauten Informationstechnik völlig neuartige Bedrohungen mit sich bringen – im schlimmsten Fall sogar Gefahren für Leib und Leben. So haben Forscher gezeigt, dass Angreifer durch Einspielen manipulierter Datenkommunikation in die internen Kommunikationsleitungen moderner Fahrzeuge (etwa durch Anklempen einer günstigen Schaltung) eine teure Reparatur eines defekten Airbagsystems gegenüber Fahrer und Werkstattpersonal überzeugend vortäuschen könnten oder sich sogar die Bremsen nach Belieben aktivieren oder deaktivieren lassen.

Angesichts dieser Bedrohungslage muss ein Sicherheitskonzept grundsätzlich aus einer abgestimmten Kombination nicht nur technischer, sondern auch rechtlicher und organisatorischer Maßnahmen bestehen. Ein wichtiges Beispiel für den nichttechnischen Bereich ist die Benutzersensibilisierung.

Zudem sollte man beim Entwurf technischer Schutzmechanismen nicht ausschließlich auf Prävention setzen – denn die wirkt nie 100-prozentig. Vielmehr sollten frühzeitig Konzepte der Entdeckung von Sicherheitsvorfällen und der Reaktion auf diese einbezogen sein. In letztere Kategorie gehören neben Bestrebungen zur Wiederherstellung eines sicheren Systemzustands durchaus auch IT-forensische Untersuchungen, um den Hergang der Vorfälle zu rekonstruieren und die Sicherheitslücken zu identifizieren und zu schließen.

Bereits vor einer Infektion des Zielsystems lassen sich insbesondere auf Ebene der technischen Infrastruktur (Pro-

vider, Betreiber von Mobiltelefonnetzen, Cloud Services, Social Networks etc.) Maßnahmen treffen, um Phänomene wie manipulierte oder sich massenhaft ausbreitende Nachrichten aufzudecken, zu überprüfen und bei Bedarf präventiv zu sperren. Beispiele sind ein konsequentes betreiberseitiges Patch-Management oder Web Application Firewalls. Aber auch Schadsoftware, die an öffentlichen Kommunikationsinfrastrukturen vorbei – mittels physischer Zugriffe – eingebracht wird, ist einzubeziehen.

Strategien der Verbreitung

Besonders für Endsysteme in modernen IT-Infrastrukturen sollte das Installieren neuer Software wirksam reglementiert sein. Hier sind die Hersteller gefragt, deren Anzahl überschaubar zu halten, auch vor dem Hintergrund der Vielzahl an Möglichkeiten, über die sich potenzielle Schadsoftware auf PC-Betriebssystemen starten lassen kann. Im Spannungsfeld zwischen maximaler Kontrolle der Anbieter und der Möglichkeit der Endnutzer für eine flexible Nutzung der Geräte und Dienste (auch abseits von Jailbreaks) stellt dies jedoch eine große Herausforderung dar. Gefragt ist ein gesunder Kompromiss zwischen Sicherheit auf der einen und Komfort auf der anderen Seite.

Für die Nutzer gelten die bekannten Ratschläge wie das Pflegen eines aktuellen Patch-Stands für Betriebssystem und Anwendersoftware oder der Einsatz von Firewalls auch weiterhin. Da präventive Maßnahmen allein angesichts des hohen Entwicklungsgrads moderner Schadsoftware und Angriffsstrategien keinen ausreichenden Schutz bieten, gewinnen wie erwähnt zunehmend Detektion und Reaktion an Relevanz. Neben den klassischen Features von Anti-Viren- und Desktop-



SAFE NEVER SLEEPS™

Sicher zu sein ist von Vorteil.
Sicher zu sein bedeutet Profit.
Sicher zu sein ist geradezu befreiend.

Aber sicher zu sein ist nicht einfach.
Besonders wenn dunkle Mächte Tag und Nacht Verschwörungen aushecken.

Es bedarf der feinfühligsten Kombination von Intelligenz und Hartnäckigkeit eines extrem effektiven globalen Teams, das Gefahren erkennt, bevor sie Schaden anrichten.

Das ist McAfee - das weltweit größte dedizierte IT-Sicherheitsunternehmen.

Digitale Sicherheit ist unser Lebenselixier. Unser Job ist es, stets einen Schritt voraus zu sein.

Effektive Sicherheit beschränkt sich heutzutage nicht auf das "wo" - es ist überall.
Jedes Endgerät, jede Verbindung, an jedem Ort, zu jeder Sekunde.

Weil wir niemals schlafen, können Sie besser schlafen.



Security

Security-Produkten bieten die Hersteller darum zunehmend integrierbare Intrusion-Detection-Module an.

Schutzprodukte können zur Identifizierung von Schadsoftware vor allem folgende Aspekte einbeziehen: typische Orte ihrer Unterbringung auf dem Zielsystem, bekannte technische Wirkungsweisen, um innerhalb dieser zu agieren, typische Selbstschutzmechanismen, typische Kommunikation mit der Außenwelt (vor allem mit dem Angreifer) und die durch sie für die Zwecke des Angreifers umgesetzten Funktionen. Technische Verfahren, um Hinweise

Obwohl Dateierkennung (statische Signaturen und Heuristiken) auch heute noch das Rückgrat vieler Sicherheitskonzepte bildet, haben schon längst andere Verfahren Einzug gehalten. Denn die signaturbasierenden Erkennungsansätze konnten mit den neuen Methoden und der schier unendlichen Anzahl der Schadsoftware nicht mehr mithalten. In der Folge entstanden statische und dynamische Heuristiken, um ohne konkrete Signatur Schutz bieten zu können. Allerdings sind auch diese Prozeduren nicht ausreichend, um auf viele moderne Bedrohungen zu reagieren – oft

einer Reputations-Cloud vereinen. Dieser Ansatz erlaubt es, auch ohne Kenntnisse über das eigentliche Objekt, anhand der Verbindungen zu anderen Objekten (Wo kommt es her? Mit wem kommuniziert es? Welche/Wie viele Nutzer kennen das Objekt?), Aussagen über das Gefahrenpotenzial zu treffen.

Eine Schutzsoftware muss heutzutage also in der Lage sein, mit verschiedenen Objekten, die Schadpotenziale bergen können, umzugehen und sie mit unterschiedlichen Techniken zu untersuchen.

Neben schadcodespezifischen Funktionen sollten

öffentlichem Adressatenkreis, und dem Nutzer so bei Bedarf Hinweise liefern.

Datenschutz nicht vergessen

Viele Herausforderungen und ungelöste Fragen betreffen nicht nur die technischen Schutzmaßnahmen, sondern rechtliche und organisatorische Aspekte. Und auch auf die Gefahr hin, zu langweilen: Besonders der Faktor Mensch sollte zukünftig noch mehr in den Vordergrund rücken. Die meisten Benutzer sind keine IT-Fachleute – und das ist

ERKENNT IHRE FIREWALL JEDEN ANGRIFF?

Deep Traffic Analytics Deep Application Control Deep Network Protection

Next Generation Firewall by Adyton Systems



Besuchen Sie uns:
auf der it-sa | Nürnberg
11. – 13. Oktober 2011
Halle 12, Stand 227

www.adytonsystems.com



auf bereits eingetretene Vorfälle auf Endbenutzersystemen zu erkennen, sind durch aktuelle Desktop-Security-Suites etwa in Form heuristischer Verhaltensanalysealgorithmen umgesetzt, die sowohl statische (aus Dateieigenschaften ableitbare) als auch dynamische Merkmale (Verhaltensmuster) einbeziehen.

Da sich die Angriffs- und Einfallsvektoren von Schadprogrammen in den letzten Jahren deutlich erweitert haben, war es unumgänglich, dass sich auch Sicherheitssoftware von rein dateibasierenden Schutztechniken zu umfassenden Schutzkonzepten entwickelte.

genug, weil sie auf die relevanten Objekte gar nicht anwendbar sind.

Ein gutes Beispiel sind Webseiten mit bösartigem Inhalt, die klassische Dateiscanner nicht analysieren können. Dafür existieren wiederum andere Ansatzpunkte zum Schutz. Eine URL ist ohne Inhaltsanalyse als bösartig markierbar, und der Zugriff darauf lässt sich verhindern, wenn bekannt ist, dass sie Schadsoftware verteilt. Auch der Inhalt ist statisch wie dynamisch auswertbar, um Exploits zu erkennen. Schließlich lassen sich die verschiedenen Techniken und das Wissen über einzelne Objekte (URLs, E-Mails, Dateien) in

moderne Security-Produkte Datenschutzrisiken untersuchen. Analog zu ersten Ansätzen aus dem Firmenumfeld (zum Beispiel Data Leakage Prevention) sollten entsprechende Funktionen auch auf Endbenutzer zugeschnitten sein. Warnungen bei bedenklichen Default-Parametern bei verbreiteten Social Networks oder Cloud-Anwendungen wären hier ein wichtiger erster Schritt. Intelligente, Content-sensitive Lösungen könnten zudem die Parameter einzelner Transaktionen bewerten, etwa bei Postings in Social Networks mit der Kombination von Keywords wie „Einladung“ oder „Party“ und

bei der Konzeption von Warnmeldungen zu berücksichtigen. Diese sollten zwar informieren, aber unnötige Stresssymptome minimieren und die Benutzer aktiv im Umgang mit dem Vorfall unterstützen. Zudem empfehlen sich organisatorische Maßnahmen zur Nutzersensibilisierung, insbesondere wenn es um Datenschutz geht. (JS)

*Tobias Hoppe, Jana Dittmann
beschäftigen sich an der
Otto-von-Guericke-Universität,
Magdeburg, mit Sicherheits-
problemen.
Maik Morgenstern
ist Mitarbeiter des AV-TEST-
Instituts.*

Kriminelle Dienstleistung

Neue Gefahren im Web 2.0

Der riesige Informationspool der vernetzten Welt ist gleichzeitig Quelle für die wichtigsten Wirtschaftsressourcen des neuen Jahrtausends: personenbezogene Nutzerdaten. Diese profitable Geldquelle aber lockt Kriminelle wie nie zuvor. Den besten Schutz vor Angriffen wie Clickjacking bietet immer noch die Vorsicht der Nutzer.

57 Millionen Deutsche haben derzeit einen Internetanschluss. Mehr als 20 Millionen sind in Online-Communities vernetzt. Das Web 2.0 revolutionierte das Internet und führte zum Aufstieg sozialer Netzwerke. Und so bringen heute auch Kriminelle Schadsoftware auf vielen verschiedenen Wegen in Umlauf.

Anders als noch vor ein paar Jahren sind infizierte E-Mails dabei nur noch vergleichsweise

wenig beteiligt. Laut Bundesamt für Sicherheit in der Informationstechnik stellen Spam-Mails mit einem Anteil von rund 96 Prozent zwar immer noch das überragende Gros des gesamten E-Mail-Aufkommens dar, sie sind jedoch längst nicht mehr so effektiv wie noch vor einigen Jahren. Die Qualität der Spamfilter sowie das Gefahrenbewusstsein der IT-Anwender haben sich verbessert – ein kleiner Teilerfolg.

Doch wo eine Gefahrenquelle langsam versiegt, tut sich eine neue, gefährlichere auf. Das Web 2.0 eröffnete viele neue Möglichkeiten – leider auch für Kriminelle. Hacking leicht gemacht: Audio- und Videomitschnitt direkt vom infizierten PC, Desktop-Streaming in Echtzeit oder die Aufzeichnung der Tastatureingaben zum Zweck des Passwortdiebstahls – mit nur wenigen Mausclicks lassen sich Trojaner für unterschiedliche kriminelle Absichten zusammenstellen. Möglich machen dies Trojaner-Baukästen, die selbst ungeübten Angreifern zu kriminellen Machenschaften verhelfen und so im Handumdrehen Tür und Tor zu sensiblen Daten Dritter öffnen. Zwischen 600 und 2000 Dollar kostet ein effektiver Baukasten in Untergrundforen, teilweise sogar inklusive 24-Stunden-Service und unbegrenzter Update-Garantie durch den „Hersteller“.

Witziges Video nicht immer lustig

Derzeit beruhen viele Hacking-Angriffe im Web 2.0 auf dem sogenannten Clickjacking.

Dabei locken Kriminelle, beispielsweise in sozialen Netzwerken wie Facebook und Twitter, mit Verlinkungen, die sich als normale Video-Posts tarnen. Diese Posts sind inhaltlich so ausgerichtet, dass sie auf ein hohes allgemeines Interesse stoßen. Im Glauben, etwas Spektakuläres wie den plötzlichen Tod von Osama bin Laden oder die Verhaftung von Christina Aguilera zu sehen, klicken zahlreiche Nutzer auf präparierte News-Meldungen. Diese geben sich gern als unverfängliche Video-Posts aus, die Absender sind in der Regel gefälscht. Opfer von Clickjacking-Attacken fragen sich im Nachhinein, wieso diese Video-Posts ausgerechnet die eigenen Freunde verbreitet haben.

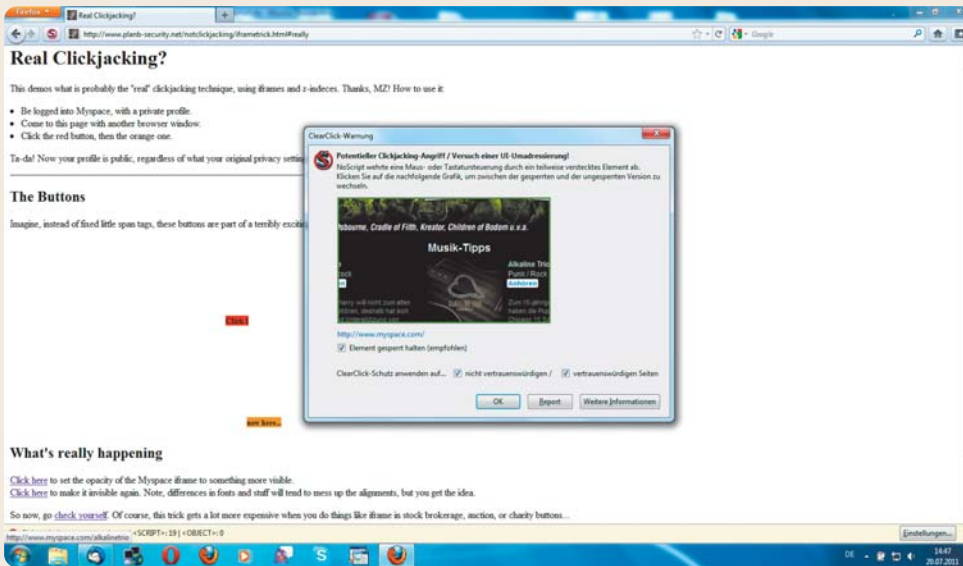
Gewöhnlich sind bei Verlinkungen auf sozialen Netzwerken wie Twitter und Facebook nicht die eigentlichen Links, sondern verkürzte Adressen wie <http://bit.ly/jdj7TK> verschickt worden. Der Empfänger kann nicht auf den ersten Blick erkennen, ob sich hinter dem URL das tatsächliche Angebot oder eine betrügerische Webseite verbirgt. Das nutzen Kriminelle aus. Klickt ein Nutzer

AIRLOCK

Geben Sie Hackern keine Chance!

Wenn es um den Schutz von Webapplikationen geht, ist Airlock Ihre beste Verteidigung. Unsere Web Application Firewall schützt Ihre Daten vor unbefugtem Zugriff. www.ergon.ch/airlock





Firefox-Plug-in NoScript schützt über eine Warnung vor Clickjacking (Abb. 1)

Quelle: Institut für Internet-Sicherheit

auf die Video-URL, gelangt der Nutzer nicht auf ein Videoportal wie YouTube, sondern auf eine präparierte Seite. Diese Seite sieht zum Beispiel YouTube zum Verwechseln ähnlich, oder die reale Internetseite ist einfach 1:1 eingebunden. Klickt der ahnungslose Nutzer nun auf das scheinbar harmlose Video, um es abzuspielen, betätigt er automatisch den „Gefällt mir“-Button“ von Facebook und wird so zur Spam-Schleuder, denn dieser Klick verbreitet den betrügerischen Link an alle Freunde.

Die Betrüger machen dabei vom sogenannten Clickjacking Gebrauch. Sie legen über den Abspiel-Button des Videos eine unsichtbare Ebene. Klickt der ahnungslose Betrachter nun auf den sichtbaren Button, spielt er nicht das Video der gezeigten Webseite ab, sondern klickt, da er sich zuvor beim sozialen Netzwerk eingeloggt hat, auf

den darübergelegten, jedoch unsichtbaren Button „Gefällt mir“. Ist der Rechner nicht mit aktuellen Sicherheits-Updates ausreichend geschützt, reicht das Aufrufen einer betrügerischen Webseite bereits aus, damit sich Schadsoftware wie ein Trojaner unbemerkt installiert. In diesem Falle spricht man auch vom Drive-by-Download.

Serverseitig besteht die Möglichkeit, dass Webanwendungen im Header das Flag „X-Frame-Options“ senden. Mit der damit verbundenen Einstellung DENY lässt sich verhindern, dass Elemente

einer Seite wie Facebook auf einer anderen Webseite eingebunden werden. Doch damit dieser Schutzmechanismus greift, muss ihn auch der Browser unterstützen. Alle aktuellen außer Konqueror berücksichtigen dies derzeit. Doch gerade eine Webanwendung wie Facebook lebt von der Einbindung des „Gefällt mir“-Buttons auf anderen Seiten und würde daher das Flag X-Frame-Options nicht nutzen.

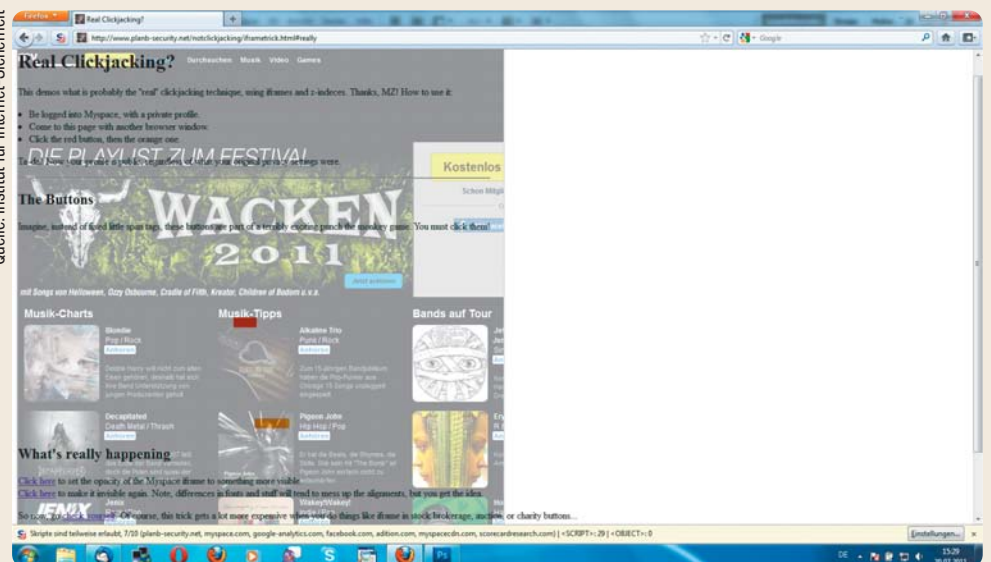
Abgesehen von serverseitigen Schutzmaßnahmen, wenn sie denn in das Konzept des Unternehmens passen, bietet bislang nur das Plug-in

NoScript für Firefox den Nutzern Schutz vor Clickjacking. Ist die darin integrierte ClearClick-Funktion aktiviert, zeigt der Browser alle verborgenen Inhalte einer Website an. Zudem sollte ein Nutzer stets hinterfragen, ob es sich um eine seriöse Verlinkung innerhalb des Newsfeed handelt. Fehlende Kommentierung und obszöne Titel der Videos können als Indizien für böartige Links dienen.

Mafia-Strukturen in der Phishing-Szene

In Zeiten, in denen ein soziales Netzwerk wie Facebook in Deutschland fast 20 Millionen Nutzer verzeichnet, boomt natürlich auch der Handel mit persönlichen Daten. Die Industrie investiert Millionen in Marktanalysen und erhofft sich möglichst genaue Profile der

Quelle: Institut für Internet-Sicherheit



Eine unsichtbare Ebene versteckt bei Clickjacking-Angriffen die tatsächliche Oberfläche der Seite (Abb. 2).

ESET SMART SECURITY 5

INTERNET SECURITY

Die neueste Kreation der Hersteller des
legendären ESET NOD32 Antivirus

Intelligente Internet-Security für
umfassenden Schutz vor:

- Bedrohungen aus dem Internet
- Hackerangriffen
- malwareverseuchten E-Mails
- infiltrierten Wechseldatenträgern
- manipulierten Webinhalten



ANTIVIRUS
ANTISPYWARE
FIREWALL
ANTISPAM
KINDERSICHERUNG


it'sa
Die IT-Security-Messe

Besuchen
Sie uns!
Halle 12,
Stand 415



www.eset.de

Best of Embedded Software Engineering – alles, was Sie für Ihr Projekt wissen müssen.

Wegen der hohen Nachfrage: 2011 erstmals auf 5 Tage verlängert! 3 Top-Keynotes und Rahmenprogramm. Über 120 Expertenvorträge und Seminare:

- Architekturdesign
- Cyber Physical Systems
- Echtzeit
- Implementierung
- Echtzeit
- GUI-Design
- Modellierung
- Multicore
- Open Source
- Sichere Software
- Software-Test und -Qualität
- Projekt-Management
- Management & Führung
- Forschung aktuell
- Fachdidaktik Softwareentwicklung

Frühbucheprerise bis 31. Oktober 2011!

Programm und Anmeldung unter: www.esk-kongress.de

07524



Embedded Software Engineering Kongress

2011

5. - 9. Dezember 2011 in Sindelfingen

Veranstalter:

ELEKTRONIK PRAXIS



MICRO CONSULT

Goldsponsoren:

Axivion
Stopping Software Erosion

Green Hills
SOFTWARE

IBM

Security

Konsumenten. Personalisierte Werbung ist das Zauberwort, das die Herzen der Marketingleute höher schlagen lässt. Von hohen Gewinnmargen ange lockt, verkaufen viele dubiose Unternehmen auf illegalem Wege beschaffte Nutzerinformationen.

Datenklau wird immer professioneller

Das Beispiel der Trojaner-Baukästen zeigt: Der Datenklau im Internet nimmt an Professionalität zu. Längst sind es nicht mehr nur die Computerge nies, die im stillen Kämmerlein an einer komplexen Spionagesoftware tüfteln. Phishing-Angriffe finden nun im großen Stil statt. Experten sprechen gar von einem wachsenden Malware-Dienstleistungssektor. Kriminelle schließen sich zu Organisationen zusammen und agieren miteinander. Ganze Netzwerke Tausender infizierter PCs entstehen und breiten sich aus.

Diese Bot-Netze instrumentalisieren die Drahtzieher als Ressourcen für weitere illegale Aktivitäten wie die Verbreitung von Spam oder dem nahezu zeitgleichen Aufrufen einer bestimmten Internetseite, um diese lahmzulegen. Jeder PC eines Bot-Netzes – im Slang als Zombie bezeichnet – führt ferngesteuert die Aktionen aus, die ihm ein sogenannter Bot-Operator übermittelt. Dabei dienen infizierte PCs beispielsweise nicht nur als Spammer, sondern auch zum Auslesen von Daten und Kennwörtern oder als Verteiler von Schadsoftware.

Damit der eigene PC nicht Opfer eines Bot-Netzes wird, ist neben dem Einsatz eines aktuellen Virenschutzprogramms und einer Personal Firewall das zeitnahe Installieren von Sicherheits-Updates nach dem Erscheinen essenziell. Damit PC-Anwender wissen, welche Sicherheits-Updates wann zur Verfügung stehen und wie sie installiert werden müssen, hat das Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen, bei dem die Autoren beschäftigt sind, den kostenlosen Warnservice „securityNews“ [1] entwickelt. Abonnenten erhalten dort kostenfrei via E-Mail oder App Informationen zum Erscheinen von Sicherheits-Updates und praktische Handlungsempfehlungen, um den akuten Gefahren bestmöglich entgegenzuwirken.

Der Wunsch nach technischem Fortschritt ist häufig größer als das Bedürfnis nach Sicherheit – eine Binsenweisheit,

die sich auf dem Sektor der mobilen Endgeräte erneut bestätigt. Der Smartphone-Markt boomt. Für 2011 prognostiziert der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) einen Absatz von zehn Millionen verkaufter Geräte. Dies würde ein Absatzwachstum von knapp 40 Prozent bedeuten. Konsumenten wünschen sich vor allem eines: grenzenlose Mobilität. Sie verstehen sich als Teil der vernetzten Welt und bewegen sich im mobilen Internet ihrer Handys genauso frei, wie sie es von heimischen Desktop-PCs her gewohnt sind: E-Mail-Datentransfer, Online-Video-Streaming und regelmäßige Statusmeldungen in sozialen Netzwerken gehören zum Alltag mobiler Internetnutzer. Dabei vergessen sie, dass die derzeitige Technik längst noch nicht so ausgereift ist, dass sie bei der Verwendung der zahlreichen Funktionen solcher Minicomputer ausreichend geschützt sind. Ein schlechter Basisschutz macht Smartphones zu leichten Angriffszielen.

Zehn Millionen leichte Angriffsziele im Web – das klingt nach einem Hacker-Eldorado. Um dies zu verhindern, sollten Anwender einige Sicherheitstipps beachten:

- Betriebssystem und Anti-Viren-Software sollten wie die installierten Apps stets auf aktuellem Stand sein.
- Sensible Daten wie die Kontaktdaten und E-Mail-Korrespondenz sollten mithilfe spezieller Verschlüsselungssoftware vor dem Auslesen geschützt sein.
- Vor dem Installieren fremder Applikationen sollte zunächst sichergestellt werden, dass es sich um eine vertrauenswürdige Software einer sicheren Quelle handelt.

Schon jetzt bieten Smartphones geeignete Schlupflöcher für Angriffe auf soziale Netzwerke, indem scheinbar nützliche Apps die Daten sozialer Netzwerke ausspionieren.

Sicherheit kommt vor Höflichkeit

Große Gefahrenherde sind außerdem die drahtlosen Schnittstellen der Geräte. WLAN, Bluetooth und Infrarot sollten aus diesem Grund nur bei tatsächlichem Bedarf aktiviert sein. Eine Verschlüsselung mittels WPA-2 und einem stark gewählten WLAN-Passwort [2] sind notwendig, sobald Nutzer eine Internetverbindung

Positivliste erwünschter Software

4ss.de

Und jeglicher unerwünschter Code ist kein Thema mehr.

SecuSurf stellt sicher, dass nur noch Code ausgeführt werden kann, der von der Administration als vertrauenswürdig eingestuft wurde. Ein Virens Scanner *erlaubt* alles außer bekannter Schadsoftware. SecuSurf *blockiert* alles außer vertrauenswürdiger beruflich benötigter Software. Auch jegliche Malware wird blockiert, sogar unbekannte. Geringer Integrationsaufwand (Bsp.: 3-5 Mann-Tage bei >5.000 PCs). Zusätzlicher Aufwand im laufenden Betrieb: Nahe Null. Webinar und Teststellung kostenlos. Muss man gesehen haben, sonst glaubt man es nicht.

über WLAN herstellen. Bitten wie „Könnte ich mal kurz Ihr Handy zum Telefonieren benutzen“ sollten die Smartphone-Besitzer generell nicht nachkommen, vor allem nicht, wenn sie das Handy beruflich verwenden. Andernfalls könnte es passieren, dass sich anschließend eine Spyware auf dem Smartphone befindet. Denn Kriminelle nutzen immer häufiger die Gutgläubigkeit der Helfer aus, um dreisten Datendiebstahl zu begehen.

Doch nicht nur der persönliche Kontakt mit Opfern eignet sich aus Sicht der Angreifer für das sogenannte Social Engineering, das gezielte Auslesen sensibler Daten unter einem scheinbar anderen Vorwand. In sozialen Netzwerken kommen zahlreiche Kontakte zustande. Mangelndes Sicherheitsbewusstsein einerseits und große Kontaktfreude andererseits führen oft zu fahrlässigem Umgang mit personenbezogenen Daten. Die Angreifer freunden sich mit Mitarbeitern eines Unternehmens an und erhoffen sich einen Informationsgewinn, der ihnen den Zugang zum Firmennetz ermöglicht. Nutzer sollten sich stets darüber im Klaren sein, welchen Adressaten sie Informationen zur Verfügung stellen. Offenherzigkeit erhöht zwar

die Aufmerksamkeit, die dem Nutzer in der Social Community entgegengebracht wird, macht ihn jedoch auch leichter angreifbar.

Reden ist nicht einmal Silber, Schweigen besser als Gold

Informationen über laufende Projekte eines Mitarbeiters oder Fotos von den Büroräumen sollten nicht für Außenstehende ersichtlich sein. Hat ein Angreifer viele Detailkenntnisse über Betriebsinterne erlangt, kann er sich beispielsweise bei einem Identitätsschwindel überzeugender als Vorgesetzter gegenüber einem Mitarbeiter ausgeben und so weitere sensible Informationen erschleichen. In jedem Fall sollten Nutzer zwischen Privatem und Beruflichem trennen. Eine Einteilung der Kontakte in verschiedene Listen, wofür neuerdings Google mit seinem neuen Netzwerk Google+ wirbt, gewährleistet, dass bestimmte Inhalte nur für ausgewählte Personen sichtbar sind.

Die Anpassung der eigenen Privatsphäre-Einstellungen ist unabdingbar, um personenbezogene Nutzerdaten auch gegenüber der Weiterverwendung durch den Anbieter der jeweiligen Social Community

zu schützen. Es gilt, stets die Motivation des Anbieters kritisch zu hinterfragen. Letztendlich läuft alles auf die Frage der Finanzierung hinaus, denn auch kostenlose Services sollen Gewinn abwerfen. Wie entstehen also Milliardenumsätze im dreistelligen Bereich bei einem kostenlosen Netzwerk wie Facebook? Millionen von Nutzern müssen finanziert werden. Sie zahlen mit ihren persönlichen Daten. Bei allem Enthusiasmus über die rasante Entwicklung im Web 2.0 darf die IT-Sicherheit nicht auf der Strecke bleiben. Persönliche Daten sind ein hohes Gut, das es zu schützen gilt.

(JS)
Malte G. Schmidt
(Diplom-Inform. FH) und
Sebastian Spooren
sind am Institut für Internet-
Sicherheit der Fachhochschule
Gelsenkirchen beschäftigt.

Onlinequellen

- [1] Warnservice des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen: www.it-sicherheit.de
- [2] Hinweise zur Sicherheit in KMU: www.kmu-sicherheit.de

Malware mit Ansage

Smartphones im Visier der Cyberkriminellen

Die Offenheit von Android- und Symbian-Systemen beim Akzeptieren von Apps aus beliebigen Quellen kann zum Fluch werden – denn sie gilt genauso für Malware. Doch auch geschlossene Systeme sind angreifbar. Anwender sollten deshalb bestimmte Regeln beachten und auf spezielle Sicherheitssoftware zurückgreifen.

Alles hatte so harmlos angefangen: ein Gerät, das Sprache und SMS übertragen konnte, dazu ein paar Telefonnummern speichern und hässliche Geräusche als Klingelton von sich geben. Und selbst diese aus heutiger Sicht sehr eingeschränkten Funktionen wurden bereits missbraucht. So gab es für ein weitverbreitetes Telefon die Möglichkeit, per SMS Funktionen zu installieren, die es zur Wanze umbauten. Bei Anruf einer bestimmten Nummer nahm das Telefon den Anruf an und aktivierte die Freisprecheinrichtung. So konnte der Anrufer alles hören, was in der näheren Umgebung ge-

sprochen wurde. Bis heute erfreut sich genau diese Funktion ungebrochener Beliebtheit in Spyware-Apps.

Spion versus Spion

Denn der Wunsch zu lauschen und die Daten zu lesen, ist nach wie vor ungebrochen. Wo früher eigentlich nur Regierungen mitmischen konnten, steht heute Spyware allen zur Verfügung: Der misstrauische Lebenspartner genauso wie der Chef ohne Skrupel und der anonyme Angreifer aus den Weiten des Internets bedienen sich dieser Apps, um an die gewünschten Daten zu kommen. Mit jeder

neuen Funktion der Smartphones wachsen die Begehrlichkeiten. Früher waren es nur Gespräche, heute sind es fast alle Details des täglichen Lebens, die sich der Interessierte per Spyware vom Telefon saugen kann, seien es der Standort, Kurznachrichten, Mails, Passwörter, Autorisierungstoken, Suchbegriffe, Tastatureingaben, Social-Networking-Beiträge, Termine, Fotos, Videos und andere Mediendaten, Dokumente auf dem Gerät und so weiter. So zentral das Smartphone für die Nutzer im Alltag geworden ist, so zentral bietet es dem Neugierigen den Zugang zu allen Aspekten des Lebens.

Reine Neugier ist leider nicht immer die Motivation. Zu wertvoll sind die Personendaten im weltweiten Datenhandel. Persönliche Zahlungsinformationen bringen bis zu zweistellige Dollar-Beträge. Auch Mail-Accounts, eBay-, Amazon- und Social-Media-Profilen spülen Geld in die Kasse. Diese von den PCs bekannten Methoden, Geld zu verdienen, erweitert das Smartphone um kostenpflichtige Service-Nummern und SMS-Dienste. So kommt das ausgerottet geglaubte Dialer-Unwesen mit den Smartphones zurück und füllt die Kassen der teilweise gut organisierten Kriminellen durch Anrufe bei diesen Nummern

oder durch Senden von SMS an eigens eingerichtete Services.

2004, fast zehn Jahre nach der ersten Malware per SMS, hat Cabir als erster Handy-Wurm das Feld neu eröffnet. Als Proof-of-Concept fragte er auf den Symbian-Telefonen, wo der Benutzer ihn selbst installieren musste, brav nach, ob er sich verbreiten dürfe.

Wer nun denkt, diese Zeiten seien vorbei, irrt. Auch heute noch fragen die meisten Malware-Programme den Benutzer um Erlaubnis. Das Sicherheitsmodell von Android und Windows Phone 7 sieht vor, dass der Anwender den Apps die Berechtigungen, die sie brauchen, ausdrücklich zuweisen muss. Wer heute Malware auf Smartphones verteilen möchte, geht zumeist den Weg des klassischen trojanischen Pferdes. Eine bekannte und beliebte, eventuell kostenpflichtige App wird um die Malware erweitert und erneut im Market oder auf anderen Download-Seiten angeboten. Besonders kostenpflichtige Apps taugen gut als Vehikel, da man dem Anwender vorgaukeln kann, er könne eine Schwarzmarkt-Version kostenfrei nutzen. Manchmal ist auch nur der Name so verändert, dass es dem Benutzer nicht auffällt.

Wenn der Anwender sie installiert hat, wird er gefragt, welche Berechtigungen die App haben solle. Wer sich jetzt nicht wundert, dass das „lustige kleine Spiel“ alle Kontakte lesen, unbegrenzt auf das Internet, die Kamera, den Standort und die SD-Karte zugreifen und sich mit den persönlichen Daten in der Cloud anmelden möchte, hat etwas später einen Trojaner installiert. Schon jetzt haben die Android-Malware „Droid Dream“ und ihre Pendanten auf den anderen Betriebssystemen dies mehrere Millionen Male getan. Genaue Zahlen stehen kaum zur Verfügung. Die über den Market heruntergeladenen Trojaner stellen einen erhebli-

ANBIETERÜBERSICHT: SICHERHEIT FÜR MOBILE GERÄTE

Anbieter	Produkt	Website
Absolute	Computrace Mobile	www.absolute.com/de
Bitdefender	Mobile Security	www.bitdefender.de
BullGuard	Mobile Security	www.bullguard.com/de
CA	Mobile Security	shop.ca.com/main/indexsca.asp
F-Secure	Mobile Security	www.f-secure.com/de/web/home_de
G Data	MobileSecurity	www.gdata.de
itWatch	DeviceWatch	www.itwatch.de
Kaspersky	Mobile Security 9	www.kaspersky.com/de
McAfee	Enterprise Mobility Management	www.mcafee.com
Secusmart	SecuSUITE	www.secusmart.com
Symantec	Mobile Security	www.symantec.com/de
TREND MICRO	Mobile Security	de.trendmicro.com/de

Auswahl ohne Anspruch auf Vollständigkeit

Security

chen Anteil. Zudem ist es viel zu einfach, unter Android Software aus Nicht-Market-Quellen zu installieren.

Märkte und Sicherheit

Die Offenheit von Android- und Symbian-Systemen, wenn es darum geht, Apps aus beliebigen Quellen zu akzeptieren, ist einerseits ein großer Vorteil bei der Entwicklung und fördert die Verbreitung. Andererseits macht man es so Anbietern von Malware sehr viel einfacher. Microsoft und Apple entschie-

ellem Fetisch oder seiner Darstellung, teilweise aber auch politische Cartoons nicht erwünscht, und die Hersteller verbieten diese in den Nutzungsbedingungen.

Nun steht es jedem Kaufwilligen frei, sich entweder für die geschlossene Welt von Apple oder Microsoft zu entscheiden oder im teilweise etwas anarchischen Chaos der Selbstregulierung bei Google sein Glück zu finden. Die geschlossene Welt bietet allerdings einige Vorzüge. So schützen sich die Geräte vor Infektionen mit Mal-

kannten Schlüssel, sodass Forensik wie auch Backup nur über Zune möglich sind.

Wer nun ganz vorsichtig ist und nur Apps installiert, die von bekannten Entwicklern mit vielen Downloads und guten Bewertungen stammen, ist dennoch nicht auf der sicheren Seite. So kann ein Angreifer über einen gehackten Entwickler-PC eine riesige Anzahl Smartphones infizieren, indem er die automatischen Updates der App um eine Malware ergänzt. Da hilft nur ein Anti-Viren-Produkt, ohne das ein

ist auch schnell ein Angreifer da, der sie ausnutzt. Früher waren für solche Attacken Telefonbücher beliebt, die über Bluetooth auszulesen waren. Heute ist das nicht mehr interessant, weil nur die Geräte in Reichweite angreifbar sind. Da sind Webseiten, die Schwachstellen im Browser oder in einer der installierten Anwendungen ausnutzen, schon effektiver, da man sie weltweit erreichen kann und die Zahl der potenziellen Opfer riesig ist. Und tatsächlich verbreiten sich Drive-By-Downloads, also

Die Kunst, sensible Daten zu schützen: SINA.

Vertrauen Sie auf die einzigartige Leistungsvielfalt von SINA. Das einzige IPsec basierte Kryptosystem mit BSI-Zulassung bis STRENG GEHEIM.

SINA (Sichere Inter-Netzwerk Architektur) ist die ganzheitliche Systemarchitektur für moderne Kryptosysteme. Entwickelt mit dem BSI für die höchsten Sicherheitsanforderungen von Behörden, Bundeswehr und geheimschutzbetreuten Unternehmen. SINA überzeugt in nationalen und internationalen Einsatzszenarien mit anspruchsvollen Sicherheitsanforderungen. Mit SINA arbeiten Sie immer sicher und effektiv: im Büro oder unterwegs.

secunet

www.secunet.com/sina

IT-Sicherheitspartner der
Bundesrepublik Deutschland

den sich für einen anderen Weg. Jede App muss über ihren Market gehen. Um eine App überhaupt dem Market hinzuzufügen, muss sich der Entwickler als Person oder Firma authentifizieren. Erst dann darf er seine Eigenentwicklung zum Begutachten vorlegen. Die Hersteller kontrollieren dann, ob die App sich an die Regeln hält, und zwar nicht nur bezüglich der Codequalität und der Berechtigungen, sondern auch inhaltliche Vorgaben betreffend. So sind üblicherweise Pornografie, jede Art von sexu-

ware durch ein nicht zugängliches Dateisystem. Datentransfer ist nur über Zune und bei Apple bis iOS 5 nur über iTunes möglich. Wer sein Android per USB an einen Rechner anschließt, sieht den externen Speicher als Wechselplatte und kann beliebig Daten jeder Art hin und her kopieren, also sein Telefon wie einen 16-GB-USB-Stick verwenden, oder Apps erst speichern und später installieren. Microsoft Phone 7 verschlüsselt eine im Telefon gefundene SD-Karte mit einem nur dem Betriebssystem be-

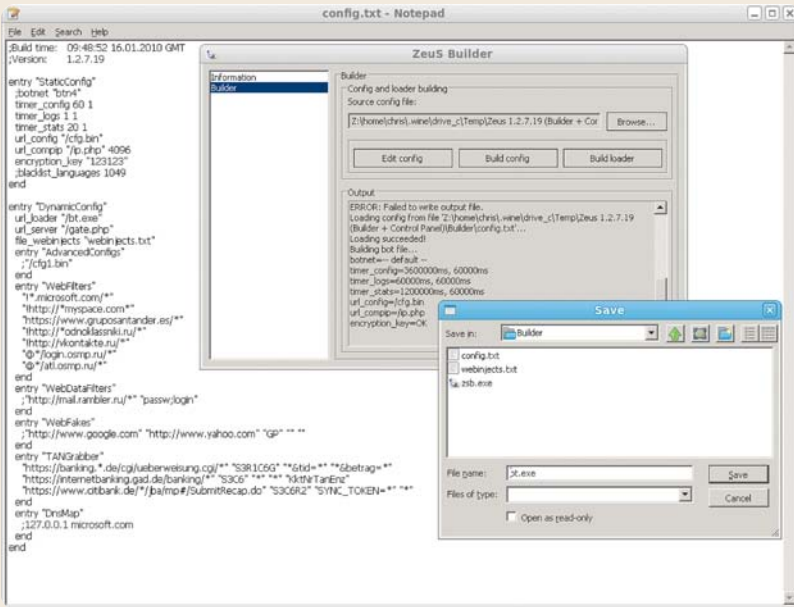
Smartphone heute genauso wenig komplett ist wie ein PC. Diese Produkte bieten natürlich auch keinen hundertprozentigen Schutz, dennoch werden bekannte und weitverbreitete Angriffe recht zuverlässig blockiert. Wer ein Komplettpaket installiert, hat dann auch gleich Backup und Remote-Wipe mit dabei.

Neben Trojanern gibt es mittlerweile auch immer mehr direkte Angriffe, sei es über Bluetooth, SMS oder den Browser. Sobald eine Schwachstelle bekannt wird,

das Installieren von Malware durch das Ausnutzen von Schwachstellen im oder um den Browser herum, auch im mobilen Umfeld immer mehr.

Spam und Phishing

Auch der Mail-Eingang auf dem Smartphone ist vor diesen Angriffen nicht sicher. Spam auf dem Smartphone stellt anders als Phishing-Angriffe keine zusätzliche Gefahr dar. Nach Auswertungen eines Phishing-Servers durch den Anbieter für sicheren Webzugang Trus-



Quelle: Puppe

Trojaner-Baukasten Zeus Builder: Oft wird den Nutzern solcher Software eine benutzerfreundliche Bedienoberfläche geboten. Keylogger- und Screenviewing-Funktion sind hier per Mausclick kombinierbar.

vor dem Zugriff gegen eine Liste bekannter Malware-URLs vergleicht und Backups ermöglicht.

Fazit

Smartphones sind vielen Risiken ausgesetzt und enthalten viele Daten, die für Angreifer interessant sind. Bei pfleglichem Umgang kann man die Funktionen der Helferlein im Alltag zu seinem Vorteil ausnutzen und die Wahrscheinlichkeit, gehackt oder elektronisch beraubt zu werden, stark reduzieren. Dennoch gilt: keine vertraulichen Informationen, keine Verchlüsselsachen oder sonstigen Geheimnisse von Firmen oder Staaten oder gefährdeten Privatpersonen sollten auf einem Smartphone lagern. Generell sollte sich jeder überlegen, seine privaten Daten zusätzlich durch eine vertrauenswürdige Verschlüsselungslösung zu schützen. (JS)

*Christoph Puppe
ist Managing Consultant und
Product Manager technical
Audits bei der HiSolutions AG
in Berlin.*

ter klicken Benutzer von Smartphones dreimal so häufig wie PC-Benutzer auf Phishing-Seiten. Dies kann unter anderem daran liegen, dass die kleinen Displays von Smartphones weniger Informationen anzeigen, der Benutzer also weniger Chancen hat, eine echte Mail seiner Bank von einer Phishing-Mail zu unterscheiden. So wird meist nur der Name des Absenders angezeigt statt Name und E-Mail-Adresse, und der Browser zeigt nur den Titel der Seite, nicht die URL inklusive Host-Namen und Gültigkeit des Zertifikats.

Umsonst ist kein Schutz zu haben

Auch hier hilft die zusätzliche Sicherheitssoftware, die mit einer Funktion für sicheres Browsen ausgestattet ist. Diese filtert alle bekannten Phishing- und Malware-URLs und warnt den Benutzer beim Besuch einer solchen. Mit einigen Maßnahmen kann der Nutzer selbst sein Gerät schützen. Das kostet allerdings Geschwindigkeit, Akkulaufzeit, Arbeit und meist auch Geld. Dennoch lohnt es sich, da jede Maßnahme zur Absicherung es einem Angreifer schwerer

macht, an die Daten heranzukommen. Folgendes sollte berücksichtigt werden:

- Komplexes Passwort vergeben,
- Verschlüsseln des Geräts, sofern möglich,
- Display-Sperre nach einer gewissen inaktiven Zeit,
- nur Anwendungen aus bekannten und überprüften Quellen installieren,

- die angeforderten Berechtigungen sehr genau kontrollieren – auch bei Updates einer App,
- Updates für das Betriebssystem und die Anwendungen sofort installieren,
- Sicherheitssoftware installieren, die jede Anwendung vor der Installation scannt, verlorene Telefone klingeln lässt und diese löschen kann, jede URL

In iX extra 11/2011:

Embedded Systems: I/O-Komponenten für die Industrie

Sensoren und Aktoren spielen in der Industrie eine große Rolle: Sie messen Umgebungsbedingungen wie Temperatur, Bewegung oder Beschleunigung und liefern so Eingabedaten für die Maschine oder die Produktionssteuerung – sei es für die Automobilindustrie,

Automatisierungs- und Medizintechnik oder Windkraftanlagen.

Dabei kommen immer neue Anforderungen auf die Systeme zu: Sensoren werden so klein, dass sie gemeinsam mit Aktoren und Steuerungselektronik auf einen Chip passen.

iX extra gibt einen Überblick über den Markt sowie die verwendeten Anschluss- und Kommunikationstechniken. Ein Ausflug in die Welt der Forschung zeigt, wohin die Reise geht.

Erscheinungstermin:
13. 10. 2011

DIE WEITEREN IX EXTRAS:

Ausgabe	Thema	Erscheinungstermin
12/11 Storage	Speicher im Netz – von iSCSI bis FCoE	17. 11. 11
01/12 Networking	Managed IT in der Cloud	22. 12. 11
02/12 Embedded Systems	Funktionale Systemsicherheit	26. 01. 12