securityNews – ein Informationsdienst für IT-Sicherheit

App goes Security

Smartphone-Apps gelten bislang in puncto Sicherheit eher als großes Risiko. Es geht aber auch anders: Das Institut für Internet-Sicherheit – if(is) hat eine securityNews-App entwickelt, die für mehr Schutz und weniger Risiko im Internet sorgen soll. Wichtigstes Anliegen dabei ist es, den Nutzer aufzuklären und mit wichtigen IT-Sicherheitsinformationen zu informieren.

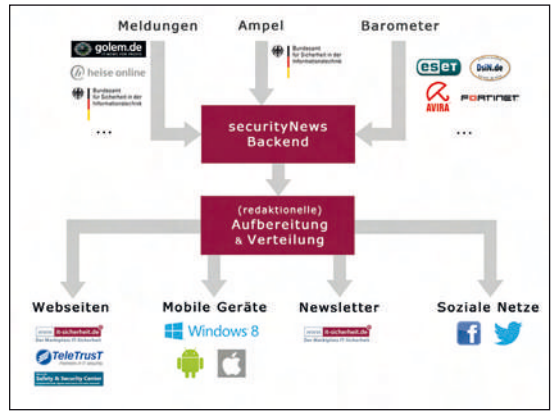
Die Gefahr durch Sicherheitslücken in weit verbreiteter Software ist allgegenwärtig. Nach aktuellen Angaben können nur rund 45 Prozent der Angriffe durch Antivirensoftware erkannt beziehungsweise verhindert werden /Syma14/. Daher ist es essenziell, dass Sicherheitslücken so schnell wie möglich geschlossen werden. Die besten Schutzmaßnahmen nutzen aber nichts, wenn der Nutzer sie nicht anwendet. Die Software-Hersteller können ihre Produkte vergeblich verbessern und patchen, wenn die Nutzer diese Patches nicht installieren. Auch im letzten Jahr waren die Verwendung nicht-aktualisierter Software und das nicht-zeitnahe Einspielen von entsprechenden Patches ein bedeutendes IT-Sicherheitsproblem, wie die Zahlen des Sicherheitsdienstleisters Secunia belegen. So waren mit Stand vom dritten Quartal in Deutschland rund 15 Prozent der verwendeten PC-Software entweder ungepatcht oder lagen in einer vom Hersteller nicht mehr unterstützten Programmversion vor /Secu13/.

Wichtige Informationen für weniger Risiko

Die zeitnahe Information der Nutzer über den Zustand ihrer IT-Geräte spielt für deren IT-Sicherheit und die Minimierung der Verwundbarkeit eine zentrale Rolle. Cyber-Kriminelle nutzen Schwachstellen in Software-Produkten mit hohem Verbreitungsgrad. Anwender spielen Updates erst Stunden oder Tage nach der Veröffentlichung auf! Der Informationsdienst „securityNews" soll das Zeitfenster zwischen dem Bekanntwerden einer Schwachstelle und dem Aufspielen von Updates klein halten. Damit ermöglicht der Informationsdienst eine Verkürzung der Handlungszeiten bis zur Reaktion auf Gefahrenlagen durch das Einspielen von Aktualisierungen oder die Deaktivierung von momentan unsicherer Software. Bei der Frage nach einem für die Darstellung und Übermittlung dieser Informationen geeigneten Medium bietet sich aufgrund der Entwicklung der letzten Jahre eine Smartphone-App an. „So besaßen im ersten Quartal 2013 bereits 62 Prozent aller Handybesitzer ein Smartphone." /Niel13/.

Es ist wichtig, die Nutzer mit richtigen IT-Sicherheitsinformationen zu versorgen, damit sie sich schneller schützen können. Und da für die meisten das Smartphone in der Tasche ein wichtiger Bestandteil des täglichen Lebens ist, auf das sie mehrmals täglich einen Blick werfen, ist es die ideale Informationsplattform. securityNews wurde als Bestandteil der vom Institut für Internet-Sicherheit initiierten Plattform „Der Marktplatz IT-Sicherheit" entwickelt. Der Marktplatz bietet IT-Sicherheitsinformationen auf verschiedene Art und Weise über diverse Kanäle an. Er wurde von Studenten und wissenschaftlichen Mitarbeitern der Westfälischen Hochschule in Gelsenkirchen entwickelt und bietet Privatanwendern und Unternehmen Zugang zu Hilfestellungen, Lösungen und weiteren Angeboten aus dem Bereich IT-Sicherheit. Mit securityNews kam ein tagesaktueller IT-Sicherheitsinformationskanal hinzu, der das Angebot auf sinnvolle Weise erweitern konnte. securityNews ist zwar auch auf der Website it-sicherheit.de abrufbar und auf eigenen Websites leicht einzubinden – die Zielplattform ist aber das Smartphone.

Zielgruppe für die App ist die Allgemeinheit. securityNews soll die breite Masse informieren, um ein flächendeckendes Bewusstsein für die Notwendigkeit von Sicherheitsupdates zu schaffen. Daher informiert securityNews auch hauptsächlich zu Updates und Sicherheitslücken bei gängiger Standardsoftware – also Betriebssysteme, Browser und beliebte Anwendungen. Die Auswahl der News erfolgt dabei durch ein am Institut ansässiges redaktionelles Team. Um der wachsenden Anzahl von Smartphones gerecht zu werden, wurde securityNews bereits für die relevanten IT-Plattformen der mobilen Geräte Apple iOS, Android und Windows 8 umgesetzt. Jede dieser Apps wurde nativ für das jeweilige System geschrieben und erfüllt so deren Richtlinien. Bei der Programmierung stand die Usability im Vordergrund, um auch Laien einen einfachen Einstieg zu ermöglichen. Außerdem werden die IT-Sicherheitsinformationen als Newsletter, über soziale Netze (Facebook und Twitter) und in einer Webansicht (Integration in jede andere Webseite möglich) verfügbar gemacht.



Übersicht des Informationsdienstes „securityNews"

Damit securityNews die gewünschte Verbreitung erreichen konnte, wurde die bewusste Entscheidung getroffen, die App kostenlos anzubieten. Das erschwert zwar die Finanzierung des Informationsdienstes, trägt aber zu einer größeren Installationsbasis und somit zu einer größeren Aufklärungswirkung bei. So wird die IT-Sicherheit im deutschsprachigen Raum verbessert. securityNews ist daher für die Finanzierung auf Fördergelder, Drittmittel und Spenden angewiesen. Die Plattform bietet drei einfache Funktionen an:

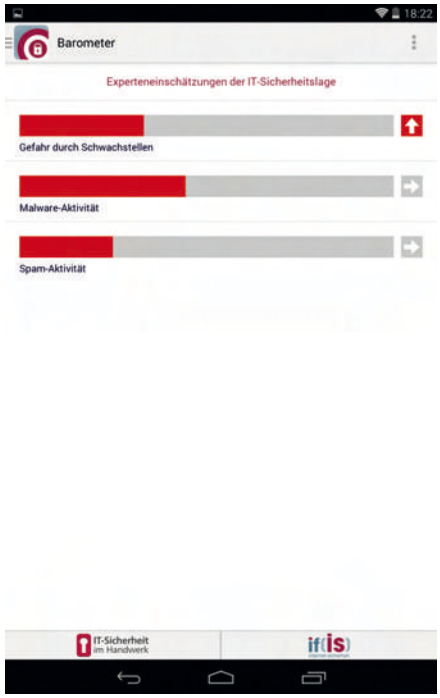
1. News: IT-Sicherheitsmeldungen über bestehende Sicherheitslücken und Updates Mithilfe der News-Funktion erreichen den Nutzer redaktionell ausgewählte IT-Sicherheitsmeldungen, die in „News" und „Up-

dates" unterteilt sind. Als News gekennzeichnete IT-Sicherheitsmeldungen informieren über akute Gefährdungen, wie z.B. bestehende Sicherheitslücken oder den Versuch von Phishing durch E-Mails, wohingegen als Update gekennzeichnete IT-Sicherheitsmeldungen über erschienene Aktualisierungen von Software informieren. IT-Sicherheitsmeldungen können verschiedenen Kategorien zugeordnet werden. Kategorien repräsentieren die gängigen Betriebssysteme „Windows", „Mac OS" „Linux" und „Mobile" zur Repräsentation mobiler Plattformen. So wird dem Nutzer die Möglichkeit gegeben, die IT-Sicherheitsmeldungen entsprechend seinen Präferenzen zu filtern. Die redaktionelle Herausforderung besteht darin, die News und Updates prägnant und verständlich zu formulieren. Die Darstellung erfolgt in einer einfachen Auflistung. Die Benachrichtigungen stehen chronologisch angeordnet untereinander, mit der aktuellsten beginnend. An der linken Seite kann der Nutzer direkt erkennen, ob es sich um eine News oder ein Update handelt. Rechts oben sind die Kategorien grafisch dargestellt. Über das Einstellungsmenü lassen sich die Kategorien schnell und einfach filtern. Gelesene News werden ausgegraut. Sie können auch durch Berühren und Halten favorisiert werden, um sie später leichter zu finden.

News

2. Barometer: Übersicht über die IT-Sicherheitslage im Internet

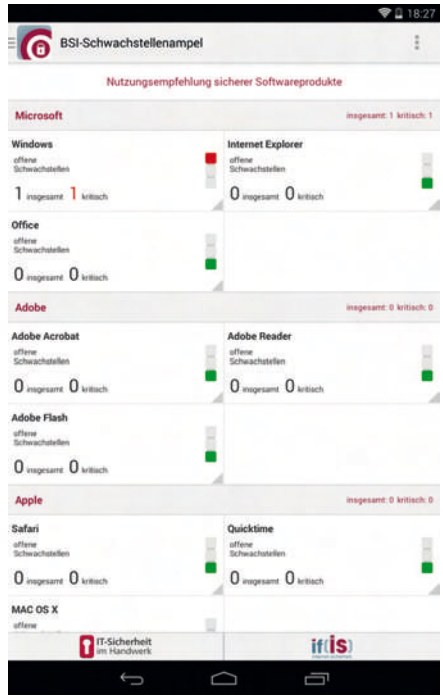
Die Funktion Barometer gibt Auskunft über die aktuelle Sicherheits- und Schwachstellenlage im Internet, jeweils von namhaften Unternehmen und Organisationen aus dem Bereich IT-Sicherheit bewertet. Ein einzelnes Barometer visualisiert dabei die prozentuale Bewertung als Balkendiagramm. Unterteilt in die Kategorien „Gefahr durch Schwachstellen", „Malware-Aktivität" und „Spam-Aktivität" werden aus den Bewertungen der Anbieter die Gesamtwertung und der Trend einer Kategorie ermittelt und diese können detailliert eingesehen werden. Das Barometer soll auf eine schnelle und intuitive Art und Weise den Nutzer über die aktuelle IT-Sicherheitslage im Internet informieren.



Barometer

3. BSI-Schwachstellenampel: Hinweis auf Sicherheitslücken in gängigen Softwareprodukten

Die Schwachstellenampel verdeutlicht die aktuelle Sicherheitslage in Bezug auf Sicherheitslücken in gängigen Softwareprodukten und ist damit eine Hilfestellung bei der aktuellen Verwendung. Die „BSI-Schwachstellenampel" wird in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik in securityNews angeboten und gibt einen Überblick über die Sicherheitslage gängiger Softwareprodukte. Der Schweregrad einer Sicherheitslücke in einem Softwareprodukt wird dabei bewertet und in einer übersichtlichen Ampeldarstellung dargestellt. Eingestuft wird dabei entsprechend der Anzahl der Lücken in „kritisch offen", „offen" ebenso wie „geschlossen" und der Schweregrad durch die Ampelfarben rot, gelb oder grün für jedes Softwareprodukt dargestellt. Auf diese Weise visuell unterstützt, kann sich der Nutzer in Sekunden informieren und einen rudimentären Überblick gewinnen. Abgedeckt werden dabei die meist verbreiteten Produkte der großen Software-Hersteller Adobe, Apple, Google, Linux, Microsoft, Mozilla und Oracle.



Schwachstellenampel

Zusammen für mehr IT-Sicherheit

Neben den vom redaktionellen Team des Marktplatzes IT-Sicherheit verfassten Meldungen sollen auch externe Partner die Möglichkeit bekommen, diese selbstständig unter einzuhaltenden Randbedienungen zu verfassen und im Rahmen eines sogenannten Anbieterkanals veröffentlichen zu können. Damit soll den Nutzern dieses Dienstes eine breitere Auswahl an Quellen angeboten werden. Die Anbieterkanäle bieten den Vorteil, dass diese Anbieter die Nutzer ohne Umwege direkt über Updates

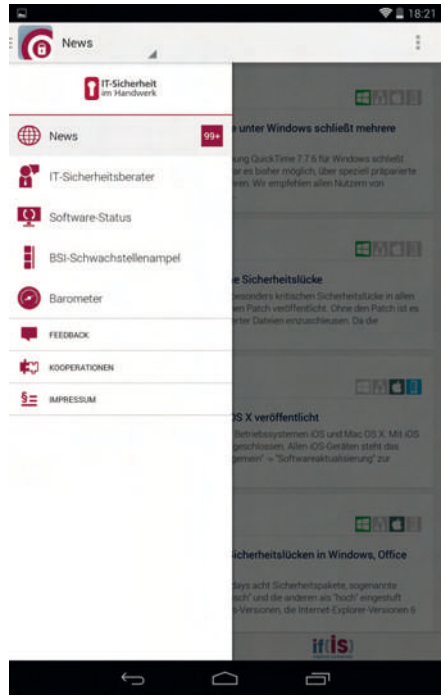
informieren können. Von der neu implementierten Funktion macht Microsoft bereits Gebrauch. Die von Microsoft herausgegebenen News und Updates erreichen den User direkt ohne einen zeitraubenden Umweg über Dritte.

Die Erstellung von Kanälen soll dabei dynamisch erfolgen, ebenso wie die freie Kategorisierung ihrer IT-Sicherheitsmeldungen durch die Anbieter selbst. Die App ist infolgedessen in der Lage, die aktuell verfügbaren Kanäle vom Server abzurufen und dem Nutzer die An- oder Abwahl neu hinzugefügter Kanäle zu überlassen. Ebenso kann der Nutzer zwischen den verschiedenen vom jeweiligen Anbieter angebotenen Kategorien wählen und somit eine Filterung nach seinem individuellen Belieben vornehmen. Für die Verwaltung von Meldungen steht den akkreditierten Anbietern eine Redakteursoberfläche zur Verfügung, die ihnen typische Funktionalitäten wie das Anzeigen, Verfassen, Bearbeiten oder Löschen sowie die Möglichkeit der Veröffentlichung bietet.

Einen weiteren Anbieterkanal bietet das Projekt „IT-Sicherheit im Handwerk" an. Das Projekt wird vom Bundesministerium für Wirtschaft und Energie gefördert und soll Handwerker für IT-Sicherheit sensibilisieren, die bislang wenig mit IT und deren Risiken in Berührung kamen. Der entsprechende Anbieterkanal enthält daher auch allgemeine Informationen über die IT-Branche sowie nützliche Sicherheitstipps und weiterführende Verlinkungen zu Anleitungen und Tutorials, mit denen jeder allein seine Computer besser schützen kann.

Spezielle Anforderungen, flexible Maßnahmen

Neben dem ohnehin vorhandenen, stetigen Streben nach Weiterentwicklung und Verbesserung der App securityNews hatte ihre Einbindung in das Projekt „IT-Sicherheit im Handwerk" im Jahr 2012 entscheidenden Einfluss auf deren Zielsetzung. Die Arbeit im Projekt zeigte schnell auf, dass eine fokussierte Zielgruppe auch spezielle Anforderungen mit sich bringt. Daher wurde mit der Arbeit an einer speziellen Version von securityNews begonnen, die weitere Funktionen mit sich brachte. Fortan steht eine erweiterte Version der App zur Verfügung, in der neben der allgemeinen Version ein zusätzliches Funktionsprofil ausgewählt werden kann, das zwei neue Funktionen bereithält.



Erweiterter Funktionsumfang für IT-Sicherheit im Handwerk

Ziel war es, innerhalb des Projekts Handwerkern und Handwerksbetrieben unter anderem regelmäßige Hilfestellungen rund um IT-Sicherheit zu geben, die ohnehin schon vorhandenen Hinweise auf Sicherheitsupdates auch an Freunde, Bekannte und Kollegen weiterzuempfehlen sowie einen PC-Sicherheitscheck anzubieten, um so mit Hilfe der App zu ermitteln, welche Software sich nicht auf dem neuesten Stand befindet und ob ein Update erforderlich ist. Aus diesen externen Anforderungen leiteten sich zwei erforderliche Erweiterungen ab, die in Form der Funktion Software-Status und der bereits genannten Anbieterkanäle realisiert wurden.

Eine der Hauptproblematiken war, dass es im Handwerk viele Menschen gibt, die ohne Unterstützung Dritter nur bedingt für die Sicherheit ihrer Software sorgen können. Veränderte Anforderungen im Beruf treffen auf bisher nicht benötigte Fähigkeiten. Um einem der Grundgedanken von securityNews nachgehen zu können, den Nutzer da abzuholen, wo er sich befindet, waren in diesem Projekt spezielle Maßnahmen erforderlich. securityNews wurde um die Funktion Botschafter/IT-Dienstleiter erweitert. Im Rahmen des Projekts sollen den Handwerksbetrieben Vertrauenspersonen an die Hand gegeben werden, die bei Prob-

lemstellungen beratend zur Seite stehen und helfen können. Um bei der Suche nach dem richtigen Botschafter/IT-Dienstleister zu helfen, wurde eine einfache Suchfunktion integriert. Es werden die in Frage kommenden Botschafter/IT-Dienstleister samt ihren Kontaktdaten angezeigt. Die Nutzer (Handwerksbetriebe, KMUs) können so schnell und direkt aus der App hinaus Unterstützung anfordern.

Eine weitere Neuerung stellt die Implementierung des Software-Status dar. Idee dabei war es, dass Nutzer bequem von ihrem Smartphone aus den Stand der Software ausgewählter PCs überprüfen können. Der Nutzer erhält also auf sein Smartphone Daten darüber, welche Software auf einem PC noch aktuell ist oder einer Aktualisierung bedarf. Mit dem Software-Status kann der Nutzer zu überwachende PCs hinzufügen, welche durch ein eindeutiges Merkmal identifiziert werden. Weiterhin hat der Benutzer die Gelegenheit, die von ihm verwalteten Systeme zu organisieren, beispielsweise durch Einteilung in Gruppen oder durch Änderung des anfangs gewählten Namens.

Die automatisierte Erfassung der installierten Software erfordert ein Programm auf dem zu überwachenden PC. Dabei wurden sowohl Drittanbieter-Lösungen sowie auch eine Eigenentwicklung in Betracht gezogen. Aufgrund des erheblichen Aufwands letzterer Option, wurde eine vorhandene Lösung ausgewählt. Die dänische Firma Secunia bietet mit dem Programm Personal Software Inspector eine kostenlose (für private Anwender) und eigenständige Lösung zur Identifizierung veralteter Software auf einem PC an. Der regelmäßige, automatische System-Scan erfasst die Versionen der installierten Programme und stuft diese als „aktuell" oder „nicht aktuell" ein. Die Ergebnisse des Scans werden in einer Übersicht zusammengefasst dargestellt und dienen dem Benutzer unterstützend bei eventuell notwendigen Handlungen. Dabei sind unter anderem folgenden Daten einsehbar:

- Zeitpunkt des letzten System-Scans,
- Anzahl der auf dem System befindlichen Programme unterteilt in aktuell, nicht aktuell und obsolet,
- Darstellung von Name, Version, Status und Zeitpunkt des letzten Scans eines Programms.

Zur sicheren Kommunikation wird am überwachten PC eine Kombination aus Token und zugehöriger Token-ID, stellvertretend für Benutzername und Passwort, generiert. Diese Kombination dient als eindeutiges Merkmal zur Identifizierung des zu überwachenden Systems und der Authentifizierung für den Zugriff auf die Schnittstelle. Dabei wird der System-Scan im XML-Format unter Verwendung von SSL/TLS verschlüsselt übertragen.

Weitere Aussichten

securityNews ist noch nicht am Ende seiner Entwicklung angelangt. Bisher implementierte Funktionen sind noch ausbaufähig, etwa die Anbieterkanäle, für die noch weitere Unternehmen und Organisationen gewonnen werden sollen. Auch die neuen Funktionen für das Projekt „IT-Sicherheit im Handwerk" stehen noch am Anfang und können in ihrem Umfang noch erweitert werden.

In Zukunft sind noch weitere Erweiterungen geplant, wie ein Video-Kanal mit nützlichen Tipps und Tutorials und ein IT-Sicherheitskalender mit Veranstaltungen und Schulungen in der Umgebung. securityNews soll sich stets an die Bedürfnisse der Nutzer anpassen und in einer sich verändernden Umwelt flexibel bleiben. So wie sich das Nutzerverhalten und die Bedrohungslage im Internet verändern, soll auch die App stets den aktuellen Anforderungen gerecht bleiben. Weitere Informationen siehe: https://www.it-sicherheit.de/securitynews/. ■

Literatur:

- */Syma14/: golem.de: SYMANTEC: „Antivirensoftware ist tot". 2014.*
- *http://www.golem.de/news/symantec-antivirensoftware-ist-tot-1405-106251.html; letzter Besuch: 29.08.2014*
- */Secu13/: Secunia ApS: Secunia PSI Country Report - Q3 2013 Germany. 2013.*
- *http://secunia.com/?action=fetch&filename=PSI-Country-Report-(DE)-(2013Q3).pdf; letzter Besuch: 29.08.2014.*
- */Niel13/: The Nielsen Company (Germany) GmbH: Deutsche legen ihr Smartphone nicht mehr aus der Hand. Webseite, 2013.*
- *http://www.nielsen.com/de/de/insights/presseseite/2013/deutsche-legen-ihr-smartphone-nicht-mehr-aus-der-hand.html; letzter Besuch: 04.04.2014.*

Benjamin Krüger (B.A.),
wissenschaftlicher Mitarbeiter im Bereich Marktplatz IT-Sicherheit am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen

Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Außerdem ist er Studienbeauftragter für den Master Internet-Sicherheit.