THE PENTEST EXPERTS.

In diesem Newsletter erwarten Sie folgende Inhalte:

Sehr geehrte Kunden, liebe Geschäftspartner, Freunde und Bekannte,

ein neues Jahr ist auch immer ein guter Zeitpunkt, Neues zu wagen. Die SySS GmbH macht in diesem noch jungen Jahr 2016 den nächsten mutigen Schritt in die Zukunft. Mit steigender IT-Vernetzung wächst gleichzeitig die Bedeutung der IT-Sicherheit. Wir wollen dabeibleiben, mit Ihnen, unseren Kunden, mitwachsen, um auch in Zukunft nicht nur konkurrenzfähig, sondern im besten Fall der erste Ansprechpartner bei Fragen rund um die IT-Security zu bleiben. Hierbei setzen wir auf eine gesunde Kombination aus langjähriger Erfahrung in der Branche, einem mutigen Bekenntnis zu Veränderungen und ständiger Neugier.

Ende Februar war es nun endlich soweit – wir haben den ersten Spatenstich für den neuen SySS-Campus auf dem ehemaligen Sidler-Areal in Tübingen getätigt. Unter den Augen zahlreicher Gäste und mit tatkräftiger Unterstützung eines humanoiden Roboters haben wir den Startschuss für unser neues „Zuhause“ gegeben und diesen natürlich gebührend gefeiert, wie Sie auf den Bildern sehen können.

An dieser Stelle ein Dankeschön an alle, die zum Gelingen dieser Veranstaltung beigetragen haben.

V.l.n.r.: Karl Stefan Schotzko, Verband f. Sicherheit i. d. Wirtschaft BW, Boris Palmer, Oberbürgermeister von Tübingen, SySS-Geschäftsführer Sebastian Schreiber und Alexander Kraus vom Bauunternehmen GOLDBECK SÜD schwingen die Spitzhacken in den Tübinger Lehmboden.

Aktuelle Events

14.-18.03.
Live-Hack auf der CeBIT 2016, Hannover

07.04.
Live-Hack Südweststrom, Tübingen

03.05.
Live-Hack ibo, Gießen

25.05.
Live-Hack Hugo Hamann, Rostock

01.06.
Live-Hack Hugo Hamann, Lübeck

07.-09.06.
Messeauftritt infosecurity, London

08.06.
Live-Hack Hugo Hamann, Kiel

15.06.
Live-Hack Hugo Hamann, Flensburg

Weitere Informationen finden Sie unter:
https://www.syss.de/pentest-blog/category/events/

Aktuelle Schulungen und Workshops

Webapp:
16. - 17.03.
01. - 02.06.

Hack2:
21. - 22.04.
29. - 30.06.

IPv6:
22.03.

Exploit:
10. - 11.05.

Windows:
05. - 07.04.

Mobile Device:
07. - 08.06.

WLAN
12. - 13.04.

Incident:
14. - 16.06.

IT-Recht:
26.04.

Pentest:
21.06.

Hack1:
19. - 20.04.
27. - 28.06.

Bei Teilnahmewunsch oder Fragen wenden Sie sich bitte an schulung@syss.de.

Impressum: SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 - 40 78 56-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Dipl.-Inform. Sebastian Schreiber
Verantwortlich für den Inhalt: Marcus Bauer · Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit. Wir werden Sie dann umgehend aus dem Verteiler entfernen.

V.l.n.r.: Alexander Kraus, GOLDBECK SÜD, Oberbürgermeister Boris Palmer und SySS-Geschäftsführer Sebastian Schreiber mit dem Modell des neuen SySS-Bürogebäudes.

Der Wachstumskurs spiegelt den Erfolg der letzten Jahre wider. Seit der Gründung der SySS GmbH im Jahre 2003 freuen wir uns an jährlich steigenden Umsätzen – im Durchschnitt 23% pro Jahr. Die personellen Kapazitäten unseres derzeitigen Firmensitzes im Tübinger Mühlenviertel sind bei diesem Aufschwung bereits erschöpft. Der Neubau stellt aber nicht allein mehr physischen Raum zur Verfügung, sondern schafft allen Mitarbeiterinnen und Mitarbeitern der SySS GmbH in meiner Erwartung auch einen deutlich erhöhten innovativen Spielraum. Die sich ständig verändernden Angriffsmuster von Hackern verlangen auch immer wieder kreative Abwehrmechanismen. Sehen Sie unseren neuen SySS-Campus somit auch als Kampfansage an Industriespione, Hacker und andere Kriminelle, um Daten und geheime Informationen unserer Kunden auch weiterhin kompetent verlässlich schützen zu können.

Wenn Sie die baulichen Entwicklungen verfolgen möchten, werfen Sie doch regelmäßig einen Blick in den neuen Bau-Blog „Building SySS“ auf unserer Homepage (https://www.syss.de/pentest-blog/category/building-syss/). Hier finden Sie natürlich wie gewohnt auch alle aktuellen Nachrichten und Informationen zum Thema IT-Sicherheit.

Herzliche Grüße,

Ihr Sebastian Schreiber

SySS-Geschäftsführer Sebastian Schreiber startet den Roboter, der den ersten Spatenstich ausführt. (Fotos: SySS)

Schadcode auf Smartphones – wie sicher sind Android-Geräte vor Angriffen?

von Roman Stühler

Im vergangenen Jahr sorgte eine Meldung über bereits vorinstallierte Malware auf verschiedenen Smartphones für Furore. Schadsoftware innerhalb des Betriebssystems ist äußerst hartnäckig und lässt sich auch nicht mehr ohne Weiteres entfernen. Fragen, die diesbezüglich immer wieder auftauchen, sind: Kann man mit einem infizierten Smartphone wirklich deren Benutzer ausspionieren und wie weit reichen diese Möglichkeiten? Neben den Auswirkungen spielt auch die Verteilung der Malware eine entscheidende Rolle. Somit bleiben weitere Fragen, so etwa: Muss ich eine derartige Schadsoftware aktiv installieren? Oder kann diese auch über andere Wege auf mein Smartphone gelangen?

Um das Ausspähpotenzial einer Applikation zu ermitteln, ist zunächst ein Blick auf das Berechtigungskonzept notwendig. Jede Android-Applikation besitzt ihren eigenen Kontext. Technisch wird dies durch einen jeweils eigenen Benutzer innerhalb des Betriebssystems realisiert. Ein Zugriff auf andere Applikationen ist somit auf einem Smartphone, welches nicht „gerootet“ ist, nicht möglich. Entwickler können einzelne Funktionen und APIs zugänglich machen, falls diese systemweit oder innerhalb der eigens entwickelten Applikationen verwendet werden sollen. Berechtigungen bezüglich eines Zugriffs auf die Android-APIs, wie die Kontaktdatenbank oder das Auslesen von Positionsdaten, müssen explizit angefordert werden. Hierfür werden die entsprechenden „Permissions“ innerhalb der sogenannten AndroidManifest.xml deklariert. Erst dann ist eine Verwendung in der Applikation möglich. Diese Berechtigungen werden bei der Installation einer App angezeigt und können auch noch nachträglich in den Applikationseinstellungen eingesehen werden. Eine Umgehung dieser Berechtigungen ist auf einem nicht „gerooteten“ Smartphone derzeit nicht möglich.

Ausgehend von einem solchen Smartphone kann eine Schadsoftware noch immer eine große Anzahl weitreichender Funktionen nutzen. Alle zu benennen, ist an dieser Stelle nicht möglich, da die entsprechenden Funktionen viel zu umfangreich sind.

Impressum: SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 - 40 78 56-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Dipl.-Inform. Sebastian Schreiber
Verantwortlich für den Inhalt: Marcus Bauer · Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit. Wir werden Sie dann umgehend aus dem Verteiler entfernen.

Die nachfolgenden Beispiele beschreiben einen gewissen Standard, der bei gängiger Schadsoftware wie „DroidJack“ oder „Androrat“ vorhanden ist und der es beispielsweise ermöglicht, die Kontakt- sowie SMS-Datenbank einzusehen, auf das Dateisystem wie die eigene Musik, Downloads oder Bilder zuzugreifen sowie den Internetverlauf des Benutzers auszulesen. Auch das Bestimmen von Positionsdaten ist selbst ohne aktiviertes GPS möglich. Hierbei werden umliegende WLAN-Netzwerke ermittelt und eine entsprechende Position trianguliert. Selbst wenn kein WLAN aktiv sein sollte, können immer noch die umliegenden Basisstationen für eine relativ genaue Positionsbestimmung genutzt werden. Neben der Möglichkeit, Vertrauliches auszulesen, können Angreifer den Betroffenen auch direkte Kosten verursachen, zum Beispiel durch sogenannte Premium-SMS-Dienste, bei denen der Angreifer eine Kurznachricht von dem entsprechenden Telefon an die angegebene Nummer verschickt. Neben diesen schon sehr bedenklichen Szenarien gibt es bedauerlicherweise aber auch Funktionalitäten, die sensible Bereiche der Privatsphäre betreffen. So kann Schadsoftware Fotos und Videos heimlich aufnehmen, ohne dass der Benutzer dies bemerkt. Im Gegensatz zu Webcams für den Computer besitzen Smartphones generell keine separate Status-LED, die eine Aufnahme signalisiert. Auch die Darstellung einer Kameravorschau wird von der API zwar vorgeschrieben, kann aber durch entsprechende Maßnahmen umgangen werden. Dies ist übrigens auch dann möglich, wenn das Smartphone sich im Standby-Modus befindet und der Bildschirm gesperrt ist.

Weiterhin können die internen Mikrofone dazu verwendet werden, Umgebungsgespräche aufzunehmen, sodass Smartphones auf diese Weise in „Wanzen“ umfunktioniert werden. Auch hier zeigen Smartphones weder auf dem Bildschirm noch bei den Symbolen oder anhand von LEDs Veränderungen an. Wie bei der Kamera können derartige Aufnahmen auch dann gemacht werden, wenn sich das Gerät im Standby-Modus befindet oder der Bildschirm gesperrt ist. Derartige Daten können anschließend verschlüsselt über HTTPS übertragen werden, was eine Analyse der Spionagetätigkeit erschwert.

Neben den bisher dargestellten, bereits erschreckenden Eingriffen in die Privatsphäre sind auch Szenarien denkbar, in denen Unternehmen gezielt ausspioniert werden. Über die aktuellen Positionsdaten kann ermittelt werden, ob sich die entsprechende Person gerade in einem Besprechungsraum innerhalb der Firma befindet. Falls dies der Fall sein sollte, könnte das stattfindende Meeting über die internen Mikrofone aufgezeichnet und im Anschluss über eine verschlüsselte Verbindung übertragen werden. Selbst wenn in dem Unternehmen mögliche Mobile-Device-Management-Lösungen bereits umgesetzt werden, die einen derartigen Zugriff vielleicht unterbinden, bleiben die Privatgeräte in den Taschen der Mitarbeiter ein Risikofaktor.

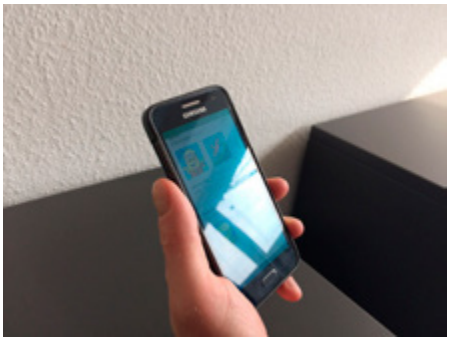

Foto: SySS

Doch wie gelangen derartige Applikationen auf mein Gerät? Die Möglichkeiten hierfür sind zahlreich. So schaffte es beispielsweise die Schadsoftware innerhalb der Applikation „Brain Test“ trotz der entsprechenden Sicherheitsmechanismen von Google bereits mehrmals erfolgreich in den Play Store. Doch auch das Ausnutzen von Sicherheitslücken, wie es bei „StageFright“ oder dem „Samsung Swift Keyboard“ möglich war, kann einen derartigen Zugriff gewähren.

Oftmals werden auch Modifikationen innerhalb bekannter Applikationen getätigt und anschließend über einen sogenannten Third-Party App Store verteilt. Die Option, welche eine Installation aus unbekannten Quellen gestattet, muss hierfür allerdings explizit aktiviert werden.

Wie bereits zu Beginn des Artikels erwähnt, besteht für einen Angreifer auch die Möglichkeit, Schadsoftware direkt innerhalb der Firmware zu platzieren, wofür dieser allerdings physikalischen Zugriff auf das Gerät benötigt. Diese entsprechende Schadsoftware verfügt über weitreichende Rechte, da dieser Systemberechtigungen eingeräumt werden können. So haben Angreifer die Möglichkeit, auf E-Mails zuzugreifen und können somit verhindern, dass der Smartphone-Besitzer Programme deinstallieren kann. Ferner ist die Schadsoftware so robust, dass sie auch nach einer Rücksetzung auf die Werkseinstellungen immer noch vorhanden ist. An dieser Stelle hilft nur das Aufspielen einer neuen Firmware. Neben den vermeintlichen Zwischenhändlern sollte dieser Aspekt auch beim Kauf von gebrauchten Smartphones berücksichtigt werden.

Auf die Frage, welche Möglichkeiten es gibt, derartige Schadsoftware zu erkennen, gibt es leider keine einfache Antwort. Generell sollte die Installation von Applikationen, die sensible Berechtigungen anfordern, ernsthaft überdacht werden. Bedauerlicherweise betrifft diese Tatsache schon einen Großteil scheinbar harmloser Applikationen. Ein Indikator für Malware könnte neben ungewöhnlichen Berechtigungen auch ein stark erhöhter Akkuverbrauch sein. Je nach Implementierung können Suchen innerhalb größerer Datenmengen oder das mehrmalige Senden diverser Informationen den Akkuverbrauch steigern. Ebenso kann ein schneller Verbrauch des entsprechenden vertraglichen Datenvolumens auf die Tätigkeit eines Angreifers hinweisen.

Impressum: SySS GmbH · Wohlboldstraße 8 · 72072 Tübingen · Tel. +49 (0)7071 - 40 78 56-0 · E-Mail: info@syss.de · http://www.syss.de · Geschäftsführer: Dipl.-Inform. Sebastian Schreiber
Verantwortlich für den Inhalt: Marcus Bauer · Sollten Sie den Newsletter nicht beziehen wollen, dann teilen Sie uns dies bitte unter newsletter@syss.de mit. Wir werden Sie dann umgehend aus dem Verteiler entfernen.