



Überblick zu den aktuellen Sicherheitsrisiken und Schwachstellen im IT-Bereich

Ivan Gudymenko

ivan.gudymenko@mailbox.tu-dresden.de

<http://wwwpub.zih.tu-dresden.de/~igudym/>

„Hacker Day“
Frankfurt, 27.11.2014



Agenda

- Aktuelle Bedrohungen und Trends: Überblick
- Kurses Demo: (Un)Sicherheit durch NFC
 - Kreditkartennummer mit NFC auslesen
- Vorschau auf die nächsten Vorträge

Wichtigste Trends im 2013

- 2013: das Jahr des „Mega Breach“
- Zunahme von gezielten Angriffen
- Zero-Day Vulnerabilities
- „Watering Holes“
- Ransomware („Strafe“ zahlen)
- Point of Sale Angriffe

[Quelle: Symantec Internet Security Threat Report 2014]

2013: das Jahr des Mega Breach

ca. 552 Mio. (!) Identities betroffen

Top-Ten Types of Information Breached

- 01 Real Names
- 02 Birth Dates
- 03 Government ID Numbers (Social Security)
- 04 Home Address
- 05 Medical Records
- 06 Phone Numbers
- 07 Financial Information
- 08 Email Addresses
- 09 User Names & Passwords
- 10 Insurance

Breaches With More Than 10 Million Identities Exposed



1

2012

+700%

8

2013

im 2012

im 2013

[Quelle: Symantec Internet Security Threat Report 2014]

Sony Pictures komplett lahmgelegt

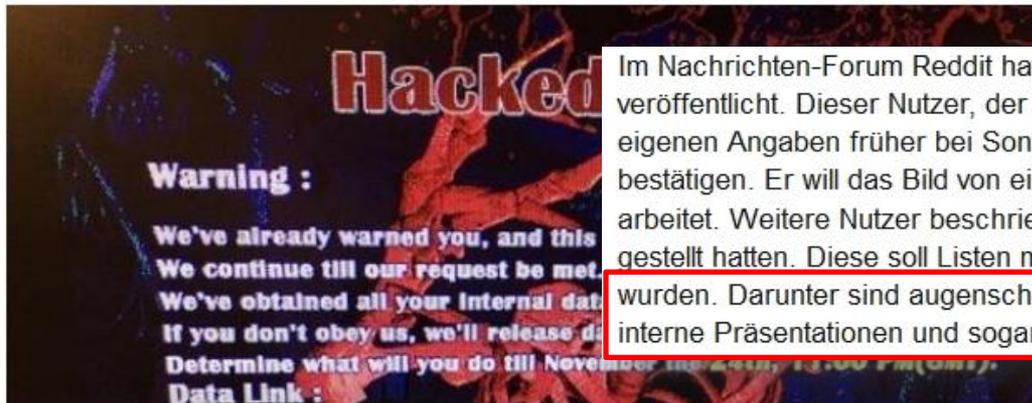
heise online > News > 2014 > KW 48 > Hacker legen Sony Pictures komplett lahm

25.11.2014 11:46

 « Vorige | Nächste »

Hacker legen Sony Pictures komplett lahm

 vorlesen / MP3-Download



Im Nachrichten-Forum Reddit hat ein Nutzer ein Foto eines gehackten Computers veröffentlicht. Dieser Nutzer, der inzwischen sein Konto gelöscht hat, hatte nach eigenen Angaben früher bei Sony Pictures gearbeitet – ältere Posts scheinen das zu bestätigen. Er will das Bild von einem Freund erhalten haben, der noch bei der Firma arbeitet. Weitere Nutzer beschrieben einer Zip-Datei, welche die Hacker ins Netz gestellt hatten. Diese soll Listen mit Dateien enthalten, die von den Hackern erbeutet wurden. Darunter sind augenscheinlich Finanzberichte, private Krypto-Schlüssel, interne Präsentationen und sogar Kopien von Pässen von Mitarbeitern.

Angreifer tauschten Android-App im Play Store aus

Die unbekanntenen Hacker sollen The Verge zufolge auch Twitter-Konten gekapert haben, die zu Sony Pictures gehören. Außerdem häufen sich Anzeichen, dass die Firma für kurze Zeit die Kontrolle über ihr Google-Play-Konto verloren hatte und jemand die App "Backup & Restore" gegen eine andere Version austauschte. Als System-App auf Sonys Xperia Handys kann man diese nicht entfernen. Die gehackte, möglicherweise bösartige App enthielt den Schriftzug "HeArT H4CK3R5" und wurde unter Umständen an einige Geräte als Update ausgeliefert. Sony hat die verdächtige App mittlerweile wieder entfernt. **betroffen sein.**

[Quelle: <http://www.heise.de/newsticker/meldung/Hacker-legen-Sony-Pictures-komplett-lahm-2462889.html>]

Zunahme von gezielten Angriffen

- Spear-Fishing: gestiegen um 93% im 2013
- U.a. durch verbessertes Social Engineering
- Angriffe über den längeren Zeitraum
 - „low and slow“ (~3 mal langsamer als im 2012)
 - weniger auffällig
- Dazu noch die „watering holes“ Angriffe (siehe weiter)

Zunahme von gezielten Angriffen (2)



[Quelle: Symantec Internet Security Threat Report 2014]

Zero-Day Vulnerabilities

- Entsteht durch die dem Vendor (noch) unbekanntem Schwachstellen in Software
- Im 2013 mehr denn je:
 - Insgesamt 23 Vulnerabilities entdeckt
 - 77% von legitimen Webseiten betroffen
 - 1 von 8 kritisch
- Mehr Möglichkeiten für „Watering holes“ Angriffe (siehe weiter)

Watering Holes Angriffe

- Erstes mal dokumentiert im 2011
- Vorgehensweise:
 - Bestimmen welche **legitime** Webseiten das Opfer (häufig) besucht
 - Injektion vom böartigen Code (Ausnutzung von Schwachstellen, u.a. auch Zero-Day)
 - Abwarten bis der Opferrechner infiziert wird
- Laut Symantec, 77% von gescannten Webseiten hatten Schwachstellen im 2013
 - 16% davon waren kritisch
 - Fazit: 1 von 8 Webpages sind unsicher!

Ransomware: Hintergrund

- „Cryptovirology“: geprägt im 1996 bei Adam Young and Moti Yung
- Hybride Verschlüsselung (kein “Reverse-Engineering” vom Schlüssel möglich)
- Hauptsächlich via E-Mail (bösender Anhang oder der Link in einer legitim aussehenden Business-Mail)

Ransomware – „Strafe“ zahlen: DE

Die offizielle Mitteilung des Bundeskriminalamtes



BUNDESPOLIZEI



Bundeskriminalamt



Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse).

Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.



Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.



ePay - Kaufen Sie Ukash in vielen tausend Supermärkten oder Call-Shops, in denen Sie dieses Logo sehen.

Achtung!

Ein Vorgang illegaler Aktivitäten wurde erkannt.

Das Betriebssystem wurde im Zusammenhang mit Verstößen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verstoß festgestellt: Ihre IP Adresse lautet "92.231.212.193" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen.

Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornographie festgestellt!

Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

Ihre Daten:

IP: [REDACTED]
Browser: Internet Explorer 7.0
OS: Windows XP
Das Land: GERMANY
City: [REDACTED]
ISP: [REDACTED]

Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen.

Die Zahlung ist innerhalb von 24 Stunden zu leisten. Sollte der Eingang der Zahlung in der vorgegebenen Zeit nicht erfolgen, so wird Ihre Festplatte unwiderruflich formatiert (gelöscht).

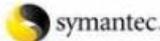
Die Bezahlung erfolgt durch einen Ukash Coupon-Code in Höhe von 100 Euro.

Um die Bezahlung durchzuführen, geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschließend auf OK (haben Sie mehrere Codes, so geben Sie Diese einfach nacheinander ein und drücken Sie anschließend auf OK)

Sollte das System Fehler melden, so müssen Sie den Code per Email (bundeskriminalamt@yahoo.com) versenden.

Nach Eingang der Zahlung wird Ihr Computer innerhalb von 24 Stunden wieder freigestellt.

Copyright 2011 Dieser Dienst des Internet Services wurde mit der Unterstützung folgender Firmen mitentwickelt:



[Quelle: http://www.homepage.eu/userdaten/0100221/709/download/anleitung_ransomware_loeschen_wheasel.pdf]

Ransomware – „Strafe“ zahlen: US

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



[Quelle: <http://blog.kiandra.com.au/2013/11/cryptolocker-time-to-take-notice/>]

Ransomware – „Strafe“ zahlen: PRISM

The image shows a ransomware lock screen with the following elements:

- Header:** Logos for the Department of Justice, FBI, and NSA. Text: "NSA INTERNET SURVEILLANCE PROGRAM PRISM COMPUTER CRIME PROSECUTION SECTION".
- Warning Bar:** "YOUR COMPUTER HAS BEEN LOCKED!"
- Message:** "Your computer has been locked due to suspicion of illegal content downloading and distribution."
- Left Panel:**
 - Text: "The illegal content (414 Mb of photo and video files) was automatically classified as child pornographic materials."
 - Text: "The downloading and distribution of illegal content, in whole or in part, violate following U.S. Federal Laws:"
 - List of laws:
 - 18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)
 - 18 U.S.C. § 2252 Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
 - 18 U.S.C. § 2252A Certain activities relating to material constituting or containing child pornography
 - Text: "Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 6 months to 10 years and shall be fined up to \$250,000."
- Right Panel:**
 - Text: "Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) §512. Thus it may be closed without prosecution. Your computer will be unblocked automatically."
 - Text: "In order to resolve the situation in an above-mentioned way you should pay a fine of \$300"
 - Illustration of a payment process: cash → card → laptop → padlock.
 - Form for MoneyPak payment:
 - Logo: "green dot MoneyPak"
 - Text: "Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:"
 - Code input field: "Code: []" with a "SUBMIT" button.
 - Buttons: "1 2 3 4 5 6 7 8 9 0" and a "x" button.
 - Status: "Status: Waiting for payment"
 - Warning: "Permanent lock on 09/28/2013 8:46 p.m. EST"
 - Text: "Where can I buy MoneyPak"
 - Logos: RITE AID PHARMACY, CVS pharmacy, Kmart, 7 ELEVEN, Walgreens, Walmart.
- Bottom Left:**
 - Section: "Collected technical data"
 - Fields: "Your IP address:", "Your host name:", "Source or intermediary sites:", "Location:" (all redacted).
 - Section: "Illegal content found:"
 - Four thumbnail images of files (all redacted).

[Quelle: <http://blog.kiandra.com.au/2013/11/cryptolocker-time-to-take-notice/>]

Ransomware: Statistiken

- Beispiel: CryptoLocker
- Anzahl der Angriffe gestiegen um 500% (!) im 2013
- Hoch profitabel
 - ca. 3% der Betroffenen zahlen die „Strafe“
 - vielleicht hatte man doch etwas zu verbergen 😊

Point of Sale Angriffe

- 60% zahlen mit einer Kredit- oder Debitkarte
- Lukratives Ziel für Angreifer



[Quelle: <http://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks>]

Ein Kurzes Demo: Kreditartennummer über NFC auslesen

Case Study: VISA PayWave mit NFC



[Quelle: <http://www.creditcardfinder.com.au/smart-cards-visa-paywave-and-mastercard-paypass.html>]

PayWave von Comdirect

Ihre Vorteile:

- **Bequem:** Zahlungen bis 25 Euro ohne PIN und ohne Unterschrift
- **Sicher:** Sie geben Ihre Visa-Karte nicht mehr aus der Hand
- **Schnell:** keine Kleingeldsuche und kein Warten auf Wechselgeld
- **Deutschlandweit:** schon über 35.000 Händler mit payWave-Terminals

Mit Ihrer comdirect Visa-Karte und der Visa-payWave-Funktion können Sie auf der ganzen Welt kontaktlos bezahlen. Nutzen Sie Ihre Visa-Karte ab sofort auch für die kleinen Ausgaben des Alltags.

Weitere Informationen

- [Info-Flyer \(PDF\)](#)

Ihre Vorteile:

- **Bequem:** Zahlungen bis 25 Euro ohne PIN und ohne Unterschrift
- **Sicher:** Sie geben Ihre Visa-Karte nicht mehr aus der Hand
- **Schnell:** keine Kleingeldsuche und kein Warten auf Wechselgeld
- **Deutschlandweit:** schon über 35.000 Händler mit payWave-Terminals

So einfach funktioniert kontaktloses Bezahlen:

Symbol auf Ihrer Visa-Karte 

Symbol an der Kasse beim Händler 

- Wenn sich ein Kontaktlos-Symbol auf Ihrer Visa-Karte befindet, können Sie Visa payWave nutzen
- Sie können bei jedem Händler kontaktlos zahlen, der das Symbol für Kontaktlos-Zahlung mit Visa-Zeichen angebracht hat
- Halten Sie Ihre Visa-Karte vor das Lesegerät
- Der Bezahlvorgang wird sekundenschnell abgewickelt
- Nutzen Sie die Visa-payWave-Funktion für Beträge bis 25 Euro sogar ohne Unterschrift und ohne PIN

[Bei diesen Händlern und Geschäften](#) können Sie schon jetzt einfach, schnell und kontaktlos mit Visa payWave bezahlen.

Kartennummer über NFC Auslesen

- Die Apps dafür sind frei verfügbar!
- Die ausgelesene Kartennummer kann missbraucht werden
 - wie etwa beim Online-Einkauf



Kartennummer über NFC Auslesen

02.07.2014 15:44

« Vorige | Nächste »

Betrug mit Online-Zugtickets: Bahn um hunderttausende Euro geprellt

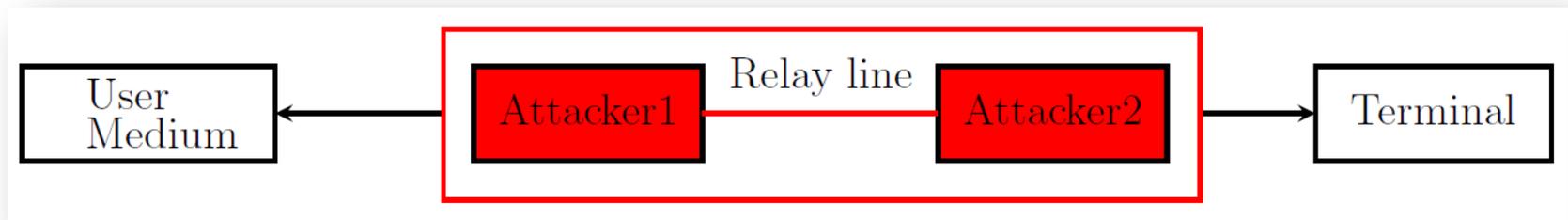
 vorlesen / MP3-Download

Die Online-Tickets wurden mit gestohlenen Kreditkartendaten bezahlt: Vier Verdächtige aus Hamburg sitzen wegen eines groß angelegten Betrugs in U-Haft. Der Schaden für die Deutsche Bahn ist hoch.

Vier junge Männer aus Hamburg sollen die Deutsche Bahn durch den Betrug mit Online-Tickets um rund 700.000 Euro geprellt haben. Die 18 bis 26 Jahre alten Verdächtigen sitzen wegen Verdachts des banden- und gewerbsmäßigen Computerbetrugs in Untersuchungshaft, wie der Sprecher der Hamburger Staatsanwaltschaft, Carsten Rinio, am Mittwoch sagte.

Kartennummer über NFC Auslesen

- Die Apps dafür sind frei verfügbar!
- Die ausgelesene Kartennummer kann missbraucht werden
 - wie etwa beim Online-Einkauf
 - ein Tracking-Merkmal
- Darüber hinaus, ein **Relay-Angriff** wäre möglich



Kartennummer Auslesen: Schutz?

- RFID-Schutzhülle
- bzw. Portmonee mit RFID-Blocker



Aktuelle Bedrohungen: Fazit

- 2013: das Jahr des „Mega Breach“
- Die Angriffe sind schlauer geworden
- Viele Webseiten sind immer noch angreifbar
- → Security IS INDEED a **Process!**

Vorschau auf die nächsten Vorträge

- (Un)Sicherheit zum anfassen: verschieden Live Hacking Demos
- Manipulierte USB-Sticks
 - Handy-Trojaner
 - SCADA-Security (Industrieanlagen)
- Hacking mit Schwerpunkt Mobile Security
 - Bösartige QR-Codes
- DDoS - Simulation eines DDoS-Angriffes

**VIELEN DANK FÜR IHRE
AUFMERSAMKEIT!**

Haben Sie noch Fragen?



»Wissen schafft Brücken.«