Alles wird gut?
Über Menschen, Angreifer und die Zukunft

Jens Liebchen - RedTeam Pentesting GmbH
jens.liebchen@redteam-pentesting.de
https://www.redteam-pentesting.de

LeetCon, Hannover, 2. November 2016

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Weltweite Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit

Penetrationstests

- Sicherheit aus der Angreiferperspektive: Kein Scan/Audit o.ä.
- Stattdessen: Individualisierte Suche, deckt gerade kritische und unerwartete Schwachstellen auf
- $\Rightarrow$ Sicherheit muss ein Gesamtkonzept sein, denn ein Angreifer sucht sich die schwächste Stelle

Mensch vs. Technik

- Penetrationstests liefern zunächst großenteils technische Ergebnisse
- Wichtigste Aufgabe ist aber: Liefern von Entscheidungsgrundlagen
  - Wie kritisch sind die Schwachstellen im Kontext? (Technik)
  - Wie können Risiken vermittelt werden? (Technik $\rightarrow$ Mensch)
  - Welche Risiken können oder sollten eingegangen werden? (Managemententscheidung)

Das Abschlussgespräch

- ★ Vorstellung und Diskussion der Ergebnisse
- ★ Sehr unterschiedliche Teilnehmer: Techniker bis hin zum Top-Level-Management
- ★ Didaktik und Psychologie spielen eine große Rolle, damit unsere Kunden im Anschluss gute Entscheidungen treffen
- ★ $\Rightarrow$ Wir begleiten unsere Kunden in absoluten Extremsituationen

Der Mensch

- ★ Im Folgenden: Typische Verhaltensweisen von Menschen und zwei interessante psychologische Effekte
- ★ Nicht nur anhand von Beispielen aus Penetrationstests
- ★ Als Techniker muss man erstmal lernen, dieses „irrationale“ Verhalten zu verstehen!
- ★ Disclaimer: Ich bin Informatiker und kein Psychologe :-)

Changes/Veränderungen

Changes/Veränderungen

Changes sind negativ.

- Menschen reagieren tendenziell negativ auf Veränderungen
- Extern ausgelöste Veränderungen, die Menschen direkt oder indirekt betreffen, werden als Angriff gewertet
- Selbst in positiven Veränderungen werden negative Begründungen gesucht

Changes/Veränderungen

Changes/Veränderungen

Changes sind negativ.

- ★ Menschen reagieren tendenziell negativ auf Veränderungen
- ★ Extern ausgelöste Veränderungen, die Menschen direkt oder indirekt betreffen, werden als Angriff gewertet
- ★ Selbst in positiven Veränderungen werden negative Begründungen gesucht

Beispiel: Mitarbeiterführung

Kommunikation Chef ⇒ Mitarbeiter

„Herr Maier, ab heute bekommen Sie pro Monat 500 Euro mehr.“

- Eindeutig positive Aussage
- Aber Gedanken von Herrn Maier:
  - Erwartet mein Chef, dass ich jetzt mehr/schneller/länger arbeite?
  - Geht es der Firma vielleicht schlecht und jetzt bleibt meinem Chef nichts anderes übrig, als mir mehr Geld zu zahlen?
  - Bekommen alle anderen etwa auch mehr Geld?
  - ...

Beispiel: Mitarbeiterführung

Kommunikation Chef ⇒ Mitarbeiter

„Herr Maier, ab heute bekommen Sie pro Monat 500 Euro mehr.“

- ★ Eindeutig positive Aussage
- ★ Aber Gedanken von Herrn Maier:
  - ★ Erwartet mein Chef, dass ich jetzt mehr/schneller/länger arbeite?
  - ★ Geht es der Firma vielleicht schlecht und jetzt bleibt meinem Chef nichts anderes übrig, als mir mehr Geld zu zahlen?
  - ★ Bekommen alle anderen etwa auch mehr Geld?
  - ...

Beispiel: Mitarbeiterführung

Kommunikation Chef ⇒ Mitarbeiter

„Herr Maier, ab heute bekommen Sie pro Monat 500 Euro mehr.“

- Eindeutig positive Aussage
- Aber Gedanken von Herrn Maier:
  - Erwartet mein Chef, dass ich jetzt mehr/schneller/länger arbeite?
  - Geht es der Firma vielleicht schlecht und jetzt bleibt meinem Chef nichts anderes übrig, als mir mehr Geld zu zahlen?
  - Bekommen alle anderen etwa auch mehr Geld?
  - ...

Beispiel: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

Beispiel: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2016_1`

Beispiel: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2016_2`

Beispiel: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2016_3`

Beispiel: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2016_4`

Beispiel: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2017_1`

Beispiel: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2017_2`

Beispiele: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

- ★ Passwort-Policy ist nichts anderes als ein Change
- ★ Einmalig definiert, aber alle drei Monate wirkend
- ★ Mitarbeiter fühlen sich gegängelt
- ★ „Als ob jemand mein Passwort raten könnte...“
- ★ Kein Verständniss, stattdessen mehr oder weniger kreative Umgehung

Beispiele: IT-Passwort-Policy

IT: Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

- ★ Passwort-Policy ist nichts anderes als ein Change
- ★ Einmalig definiert, aber alle drei Monate wirkend
- ★ Mitarbeiter fühlen sich gegängelt
- ★ „Als ob jemand mein Passwort raten könnte...“
- ★ Kein Verständniss, stattdessen mehr oder weniger kreative Umgehung

Klassische IT als Quelle für Changes

Die klassische IT-Abteilung wird schnell als Quelle für Changes ausgemacht:

- ★ Policies stammen von der IT
- ★ Adressierte Probleme sind abstrakt und nicht nachvollziehbar
- ★ Maßnahmen werden technisch begründet
- ★ Changes sind unvermeidbar: OS-Updates, große Rollouts. . .
- ★ Geht ein Change schief, fühlen sich die Nutzer in ihrem negativen Bild bestärkt

Binäres Denken

Binäres Denken

Menschen tendieren dazu, nur schwarz-weiß zu denken.

- „Ich vertraue meinen Kollegen, warum soll da noch über Zugriffskontrolle gesprochen werden?“
- „Was bringt eine Firewall, wenn Mitarbeiter angegriffen werden können?“
- Nach Snowden-Veröffentlichungen:
  - Resignation („Jetzt ergibt ja alles keinen Sinn mehr.“)
  - Aktionismus („Wir müssen uns vor der NSA schützen!“)

Binäres Denken

Binäres Denken

Menschen tendieren dazu, nur schwarz-weiß zu denken.

- „Ich vertraue meinen Kollegen, warum soll da noch über Zugriffskontrolle gesprochen werden?“
- „Was bringt eine Firewall, wenn Mitarbeiter angegriffen werden können?“
- Nach Snowden-Veröffentlichungen:
  - Resignation („Jetzt ergibt ja alles keinen Sinn mehr.“)
  - Aktionismus („Wir müssen uns vor der NSA schützen!“)

Binäres Denken

Binäres Denken

Menschen tendieren dazu, nur schwarz-weiß zu denken.

- „Ich vertraue meinen Kollegen, warum soll da noch über Zugriffskontrolle gesprochen werden?“
- „Was bringt eine Firewall, wenn Mitarbeiter angegriffen werden können?“
- Nach Snowden-Veröffentlichungen:
  - Resignation („Jetzt ergibt ja alles keinen Sinn mehr.“)
  - Aktionismus („Wir müssen uns vor der NSA schützen!“)

Binäres Denken

- ★ Binäres Denken blockiert lösungsorientiertes Handeln
- ★ 100%-Lösungen existieren nicht
- ★ Resignation und Aktionismus gefährdet Unternehmensfortbestand

Abschlussgespräche in Penetrationstests

- ★ Es wird nur über Schwachstellen und damit über Changes gesprochen
- ★ Reaktionen sind zeitkritisch
- ★ Ziel: Management und Techniker treffen gemeinsam bestmögliche Entscheidungen
- ★ Hierbei darf weder in Resignation noch in Aktionismus verfallen werden

„Der Angreifer“

- ★ Angreifercharakterisierungen sind zahlreich
- ★ Sollte ein Unternehmen überhaupt Angst vor einem Script-Kiddie haben?
- ★ Wie verhält sich ein ernstzunehmender Angreifer?

Ernstzunehmende Angreifer

Ernstzunehmende Angreifer verhalten sich ähnlich wie jedes andere Unternehmen:

Return on Investment (ROI)

$$ROI = \frac{net\ income}{investment}$$

- ★ Risiken werden abgewogen
- ★ Vorgehen ist oft arbeitsteilig
- ★ Teilweise werden „Arbeiten“ sogar ausgeschrieben

ROI als Motiviation

Eine Charakterisierung mit Hilfe des ROI ist nicht neu:

- ★ Ungerichtete Einbrüche vs. gezielte Einbrüche
- ★ Gewinn-/Abo-Betrug vs. Enkeltrick und Chefmasche
- ★ Arbeitsteiliges Vorgehen selbst bei einfachen Taschendiebstählen

Erpressung von Online-Anbieter

- ★ Erpressungen von Online-Anbietern finden seit Jahren statt
- ★ Meistens kurzfristiger Angriff per DDoS, dann Forderung
- ★ Bedrohung der Verfügbarkeit zu Spitzenzeiten
- ★ Zahlungen im niedrigen fünfstelligen Euro Bereich
- ★ Problem: Viele Anbieter zahlen

Aufwand, Risiko und Ertrag der Erpresser

- ★ Aufwand: Vorbereitung, Bot-Net, Zahlungsabwicklung
  ⇒ Eher gering
- ★ Risiko: Firmen versuchen, Angreifer zu identifizieren
  ⇒ Potentiell finanzkräftiger Gegner, aber Risiko trotzdem überschaubar
- ★ Ertrag:
  ⇒ lohnenswert
- ★ Aber: „Geschäftsmodell“ skaliert nicht

Aufwand, Risiko und Ertrag der Erpresser

- ★ Aufwand: Vorbereitung, Bot-Net, Zahlungsabwicklung
  ⇒ Eher gering
- ★ Risiko: Firmen versuchen, Angreifer zu identifizieren
  ⇒ Potentiell finanzkräftiger Gegner, aber Risiko trotzdem überschaubar
- ★ Ertrag:
  ⇒ lohnenswert
- ★ Aber: „Geschäftsmodell“ skaliert nicht

Aufwand, Risiko und Ertrag der Erpresser

- ★ Aufwand: Vorbereitung, Bot-Net, Zahlungsabwicklung
  ⇒ Eher gering
- ★ Risiko: Firmen versuchen, Angreifer zu identifizieren
  ⇒ Potentiell finanzkräftiger Gegner, aber Risiko trotzdem überschaubar
- ★ Ertrag:
  ⇒ lohnenswert
- ★ Aber: „Geschäftsmodell“ skaliert nicht

Aufwand, Risiko und Ertrag der Erpresser

- ★ Aufwand: Vorbereitung, Bot-Net, Zahlungsabwicklung
  ⇒ Eher gering
- ★ Risiko: Firmen versuchen, Angreifer zu identifizieren
  ⇒ Potentiell finanzkräftiger Gegner, aber Risiko trotzdem überschaubar
- ★ Ertrag:
  ⇒ lohnenswert
- ★ Aber: „Geschäftsmodell“ skaliert nicht

Ransomware/Krypto-Trojaner

Ransomware/Krypto-Trojaner

Ransomware: US-Polizisten zahlen Lösegeld für ihre Daten

Corbis

Technik im Polizeiauto: Die Polizisten überwiesen den Erpressern Bitcoin

Eine amerikanische Polizeistation ist Opfer eines Lösegeld-Trojaners geworden. Doch statt ruhig zu bleiben, zahlten die Polizisten rund 600 Dollar an die Erpresser. Dabei hätte es vielleicht eine viel einfachere und preiswertere Lösung gegeben.

Quelle: `http://spon.de/aervi`

Ernstzunehmender Angreifer?

Ernstzunehmender Angreifer?

- ★ Ein Angreifer hat bliebigen Programmcode auf Ihrem Rechner ausgeführt und hatte Zugriff auf wichtige Daten
- ★ Diesen Angriff haben Sie bemerkt...
- ★ ...leider aber nur, weil der Angreifer es so wollte!

⇒ Andere Angriffe bemerken Sie normalerweise nicht so einfach!

Ernstzunehmender Angreifer?

- ★ Ein Angreifer hat bliebigen Programmcode auf Ihrem Rechner ausgeführt und hatte Zugriff auf wichtige Daten
- ★ Diesen Angriff haben Sie bemerkt...
- ★ ...leider aber nur, weil der Angreifer es so wollte!

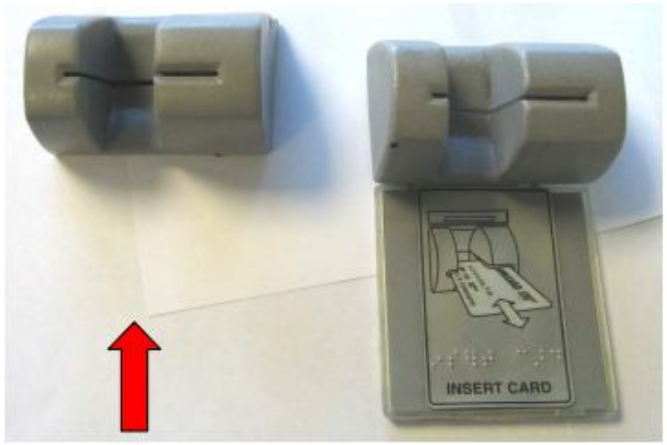
⇒ Andere Angriffe bemerken Sie normalerweise nicht so einfach!

Ernstzunehmender Angreifer!

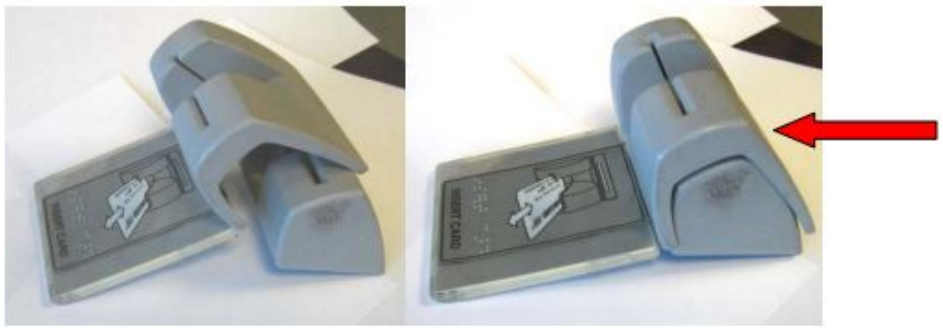
„Law 1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore. “

(10 Immutable Laws of Security, Microsoft)

Angriffe auf Bankautomaten und Kartenzahlungen



The real card reader slot. The capture device



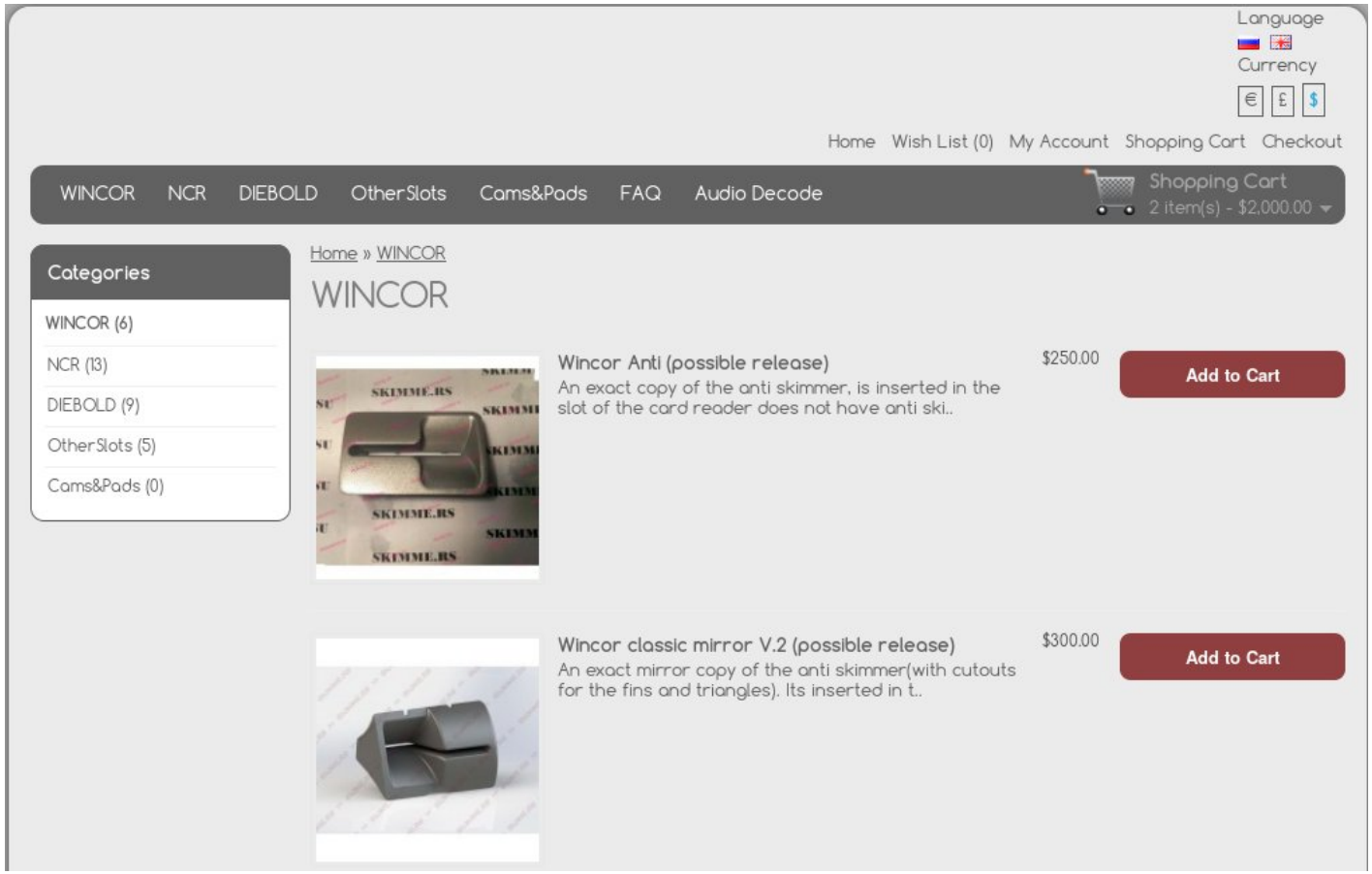
The side cut out is not visible when on the ATM.

Quelle: `https://krebsonsecurity.com/`

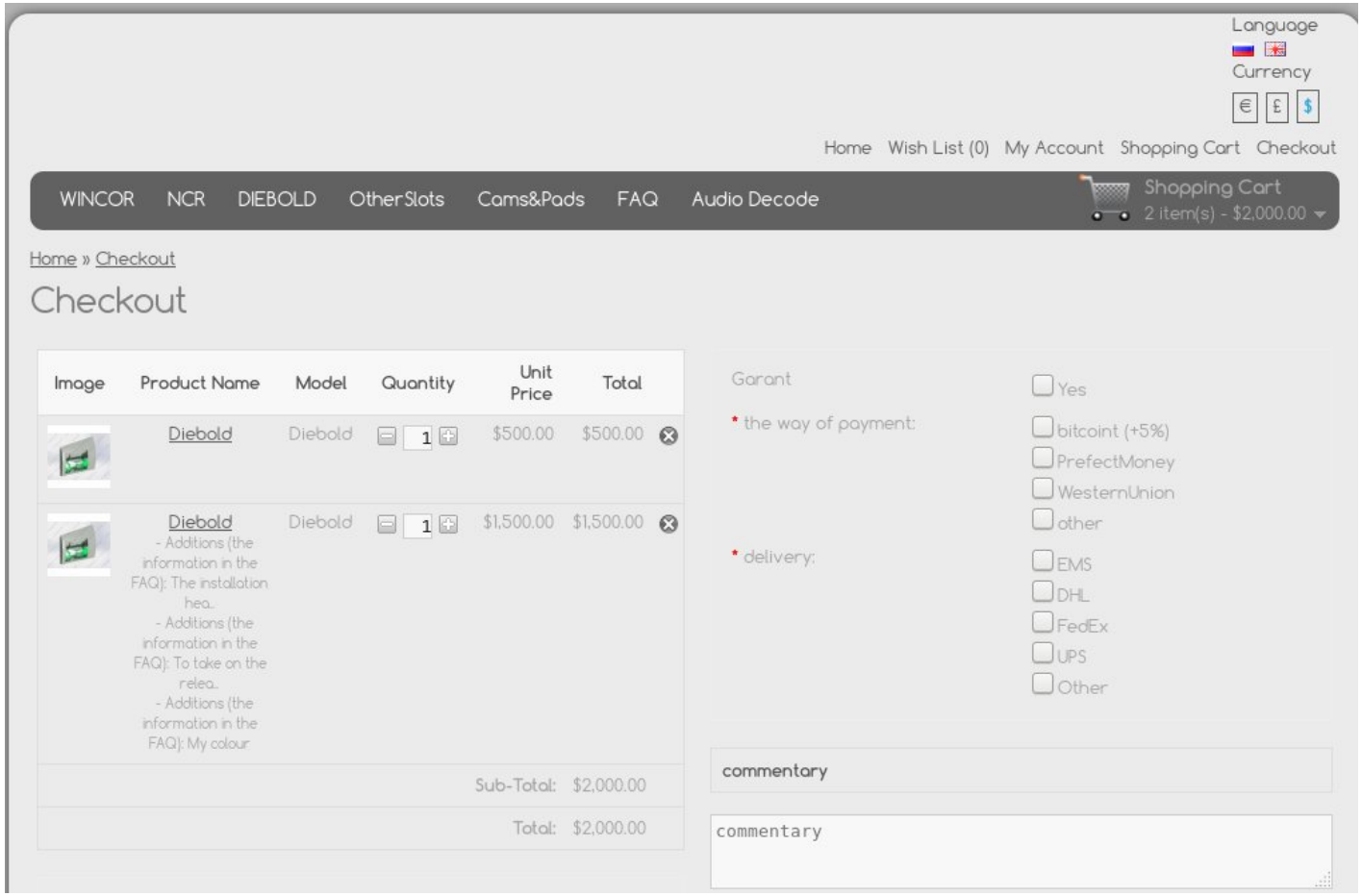
Angriffe auf Bankautomaten

Quelle: `https://www.europol.europa.eu`

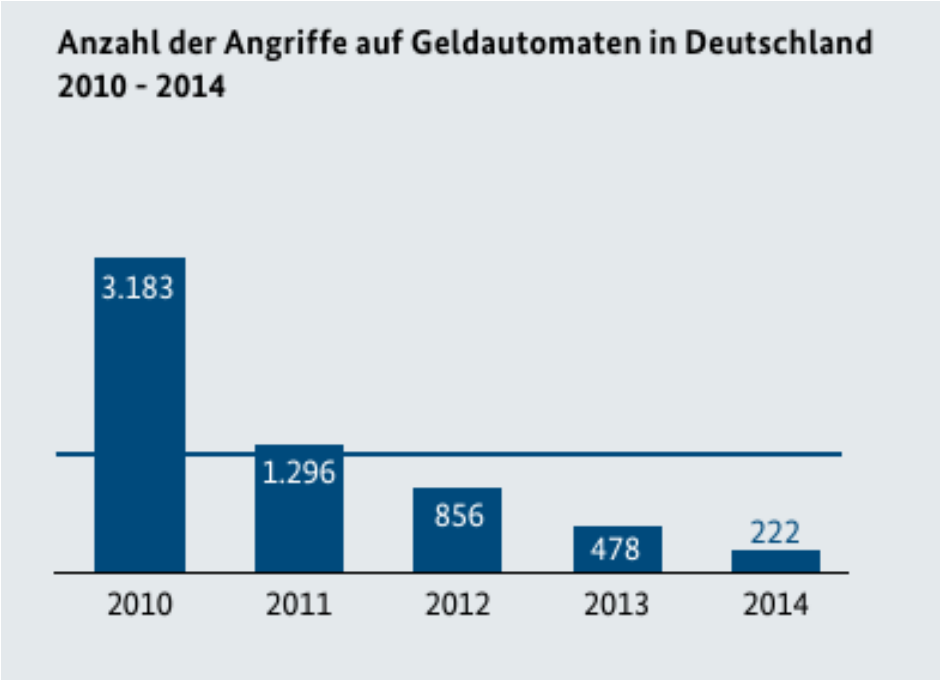
Angriffe auf Bankautomaten



Angriffe auf Bankautomaten



Aufrüstung der Banken



Quelle: Bundeskriminalamt Bundeslagebild Zahlungskartenkriminalität 2014

Angriffe auf POS-Terminals

20 ° / 13 °
Regenschauer

Hannoversche Allgemeine

START | NACHRICHTEN | HANNOVER | THEMA | BILDER | VIDEOS | sonntag | FREIZEIT | RATGEBER | ANZEIGEN | ABO & LESERSERVICE | INHALT

Aus der Stadt | Aus den Stadtteilen | Aus der Region

HAZ › Hannover › Aus der Stadt › Übersicht › Betrüger plündern Konten von 140 Baumarktkunden in Hannover

Abo bestellen › | HAZ-Shop › | HAZ Media Store › | AboPlus › | HAZ Service ›

Datenklau

Kommentieren | Drucken | Text + −

Betrüger plündern Konten von 140 Baumarktkunden in Hannover

In Hannover gibt es einen neuen Fall von Datenklau: Nachdem zwei Geldautomaten der Volksbank manipuliert worden sind, haben Betrüger nun auch ec-Kartenleser im Hornbach-Baumarkt präpariert – die Geräte stehen direkt an der Kasse.

VORIGER ARTIKEL
Hannover feiert sein Europaspiel

NÄCHSTER ARTIKEL
„BootBooHook"-Festival startet in neuer Dimension

Von Michael Soboll

Artikel veröffentlicht: Donnerstag, 18.08.2011 07:16 Uhr

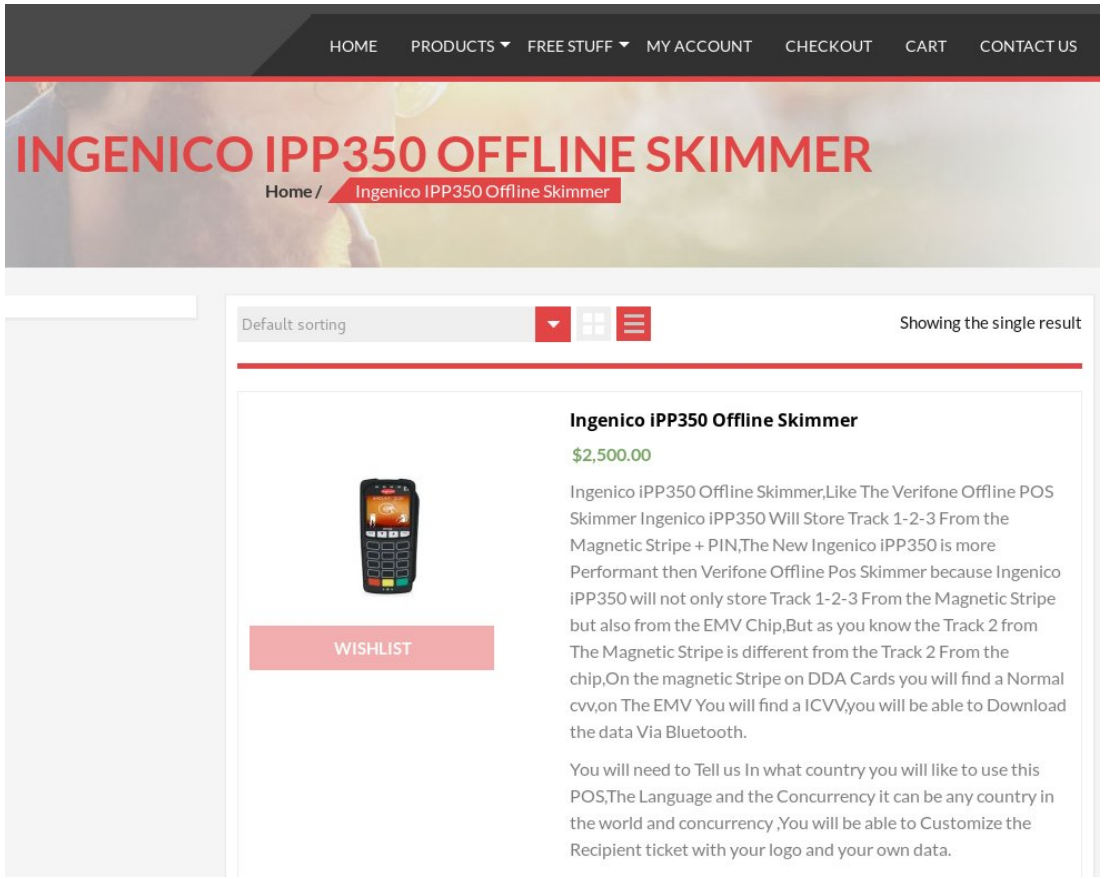
Artikel aktualisiert: Donnerstag, 18.08.2011 07:24 Uhr

Im Hornbach-Baumarkt auf dem Hanomag-Gelände in Linden wurden die Kontodaten der Kunden mit einem perfiden Trick ausgespäht.

Quelle: Rainer Surrey

Quelle: Hannoversche Allgemeine `http://www.haz.de`

Angriffe auf POS-Terminals



Angreifer in der Praxis?

Angreifer in der Praxis

- ★ Im Allgemeinen: Vergessen Sie „Cyber“ und „APT“!
- ★ Konzentrieren Sie sich auf für Sie realistische Angreifer
- ★ Nutzen Sie den ROI für Ihre Überlegungen
- ★ Verfallen Sie weder in Aktionismus noch in Resignation

IT-Sicherheit

⇒ Treffen Sie vernünftige unternehmerische Entscheidungen!

Angreifer in der Praxis

- ★ Im Allgemeinen: Vergessen Sie „Cyber“ und „APT“!
- ★ Konzentrieren Sie sich auf für Sie realistische Angreifer
- ★ Nutzen Sie den ROI für Ihre Überlegungen
- ★ Verfallen Sie weder in Aktionismus noch in Resignation

IT-Sicherheit

⇒ Treffen Sie vernünftige unternehmerische Entscheidungen!

Ein Blick in die Zukunft

Betroffene Branchen

Angriffe werden auf bisher nur wenig betroffene Branchen ausgeweitet werden:

- ★ Es wird gerade die Branchen treffen, bei denen IT nur Mittel zum Zweck ist
- ★ Insbesondere Medizinsektor wird betroffen sein
- ★ Angriffe werden zu Kollateralschäden führen
- ★ Mehr Angriffe werden öffentlich werden, da Folgen dramatisch und öffentlich
- ★ Angriffe werden teilweise öffentliche Sicherheit und Ordnung gefährden

Internet of Things

Angriffe auf IoT-Devices werden zum Volkssport:

- ★ Angriffe aus „Spaß-am-Gerät“
- ★ Fernseher, Heizungsanlagen und andere smarte Geräte werden anfangen, Lösegeld zu fordern

Die Menschen

- Bevölkerung beginnt diffuse Ängste zu entwickeln
- Industrie bemerkt Abhängigkeit und Unkontrollierbarkeit bei laufenden Angriffen
- Staaten reagieren mit starren Regeln und mehr Überwachung
- Menschen reagieren privat zweigeteilt:
  - IT-Sicherheit und Updates werden zum Kaufargument
  - Teilweiser Rückzug von smarten Geräten

Ethik

- ★ Es gibt in der praktischen Informatik immer mehr Fragen, die sich nicht mehr eindeutig mit Ja oder Nein beantworten lassen
- ★ Ethik wird in Zukunft eine wichtige Rolle spielen

Ethik in Penetrationstests

Einige Beispiele aus Penetrationstests:

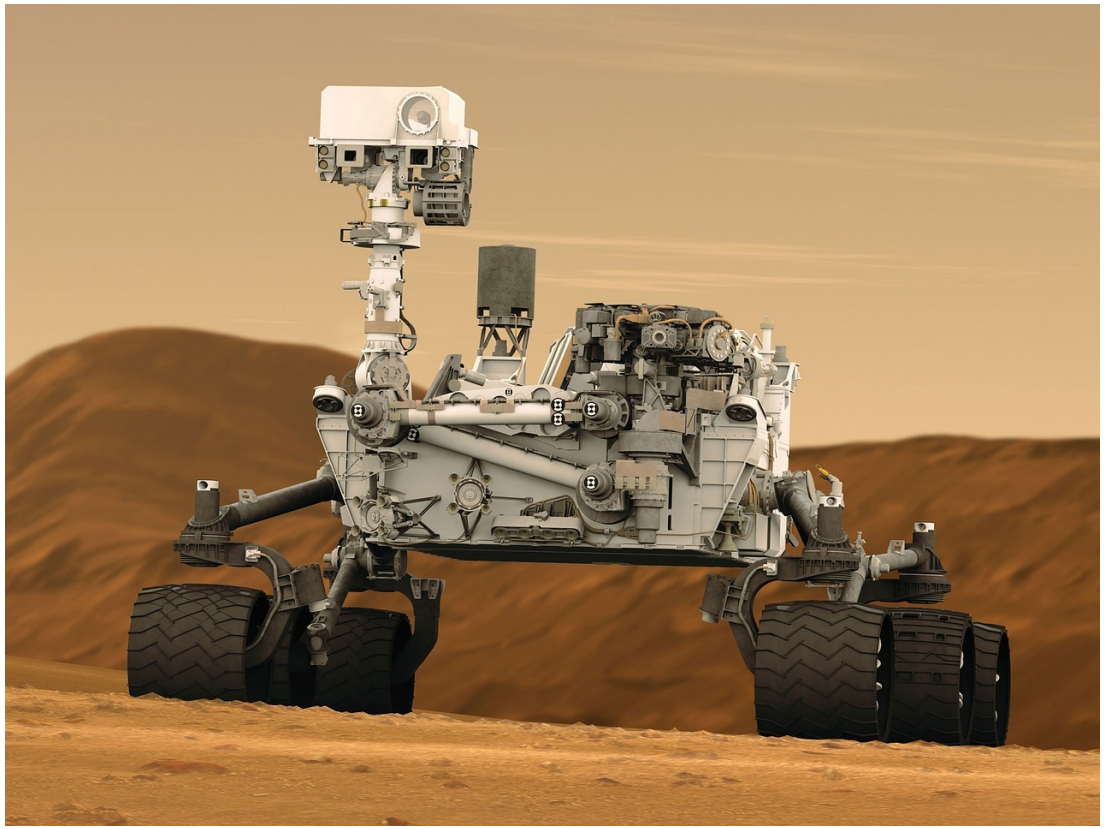
- ★ Darf ein Penetrationstester ein E-Mail-Archiv einsehen und z.B. nach Passwörtern durchsuchen?
- ★ Im Penetrationstest gelingt ein Zugriff auf das AD. 95 % der Passworte sind schwach und können gefunden werden. Sollen/Müssen/Dürfen diese Passwörter in den Bericht?

Ethik in Penetrationstests

Einige Beispiele aus Penetrationstests:

- ★ Darf ein Penetrationstester ein E-Mail-Archiv einsehen und z.B. nach Passwörtern durchsuchen?
- ★ Im Penetrationstest gelingt ein Zugriff auf das AD. 95 % der Passworte sind schwach und können gefunden werden. Sollen/Müssen/Dürfen diese Passwörter in den Bericht?

Autonomes Fahren



Autonomes Fahren

„Zwei Grundsätze sollten dabei klar sein: Sachschaden geht immer vor Personenschaden. Und es darf keine Klassifizierung von Personen geben, etwa nach Größe oder Alter.“

Bundesverkehrsminister Alexander Dobrindt, Bild-Interview 9.07.2016

Autonomes Fahren

- ★ Erkauft sich ein Fahrer eines Oberklassewagens nicht bereits einen Vorteil bei einem Crash gegen ein kleineres Fahrzeug?
- ★ Schon heute führen Assistenzsysteme zu anderen Unfällen und anderen Unfallbeteiligten
- ★ Kein Fahrer kann in Extremsituationen wirklich abwägen. Computer werden es können.
- ★ Die Frage ist: Soll ein Computer dann wirklich würfeln? Oder soll er doch abwägen?
- ★ Wer ist für die Abwägung verantwortlich? Und wer kann sie noch beeinflussen?

Autonomes Fahren

- ★ Erkauft sich ein Fahrer eines Oberklassewagens nicht bereits einen Vorteil bei einem Crash gegen ein kleineres Fahrzeug?
- ★ Schon heute führen Assistenzsysteme zu anderen Unfällen und anderen Unfallbeteiligten
- ★ Kein Fahrer kann in Extremsituationen wirklich abwägen. Computer werden es können.
- ★ Die Frage ist: Soll ein Computer dann wirklich würfeln? Oder soll er doch abwägen?
- ★ Wer ist für die Abwägung verantwortlich? Und wer kann sie noch beeinflussen?

Ethik

- ★ Hersteller werden sich Wettbewerbsvorteile über eigene „Ethik“ verschaffen
- ★ Beispiel: Sicheres Auto, welches Insassenschutz priorisiert
- ★ Ethische Grenzen der Technik werden herstellerseitig teilweise ignoriert werden
- ★ Ethische Grenzen werden im Bewusstsein der Menschen ankommen

Autonomes Fahren

„If you know you can save at least one person, at least save that one. Save the one in the car.“

Christoph von Hugo
Mercedes's Manager of
Driver Assistance Systems, Active Safety and Ratings
Paris Motorshow 2016

Bug-Bounties

- Bug-Bounties werden zu verstärkten Marktaktivitäten im Grau- und Schwarzmarkt führen
- Wirklich interessante Schwachstellen werden den betroffenen Herstellern im Rahmen von eigenen Bug-Bounties nicht mehr gemeldet werden

Bug-Bounties

Hersteller können bei Bug-Bounties auf Dauer kaum gewinnen:

- ★ Hersteller kann maximale Prämie nur anhand des ROI des betroffenen Produktes bestimmen
- ★ Dritte zahlen anhand der mit dem Produkt geschützten Daten $\Rightarrow$ Betrag ist höher
- ★ Dadurch, dass Hersteller auch große Summen zahlen, werden mehr Leute motiviert, überhaupt zu suchen
- ★ Diese verkaufen ihre Ergebnisse dann aber an Dritte

Fazit

Alles wird gut?

Fazit

Nicht alles wird schlecht!

- ★ Kümmern Sie sich (ohne Aktionismus) um die für Sie relevanten Angreifer!
- ★ Leben Sie mit Risiken!
- ★ Verpassen Sie keine Innovationen, weil sie vorschnell resigniert ablehnen!
- ★ Gehen Sie aber auch keine unnötigen Risiken ein!

Zeit für Fragen und Diskussionen

Vielen Dank für Ihre Aufmerksamkeit