Sicherheit und Industriespionage – Von technischen und menschlichen Schwächen

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

Veranstaltung Datensicherheit, IHK Aachen, 25. April 2012

RedTeam Pentesting, Daten & Fakten

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

Zusammenhang Penetrationstests und Industriespionage

- ★ Kunden berichten immer wieder über Fälle von Industriespionage
- ★ Auch kleine Firmen sind betroffen (mehr als die meisten vermuten)
- ★ Aggressive „Wettbewerbsanalysen“ nehmen zu
- ★ Denken Sie bei außergewöhnlichen Vorkommnissen (Umsatzrückgang, auffallend gut/schlecht passende Bewerber etc.) auch an Industriespionage!
- ★ Handeln Sie vorbeugend, gerade kleine Firmen haben oft Probleme, einen Ausfall zu kompensieren!

Wie kommt ein Angreifer an unsere Daten?

- ★ Sicherheit muss ein Gesamtkonzept sein, denn ein Angreifer sucht sich die schwächste Stelle
- ★ Im Folgenden: Interessante Schwachstellen gerade abseits der klassischen technischen Schwachstellen

Social Engineering

„Social Engineering [...] nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen.“

(Wikipedia)

Faktor Mensch

Warum sind Social Engineering-Attacken erfolgreich?

- ★ sensitive Informationen oft nicht intuitiv als solche erkennbar
- ★ spontane Einschätzung von Risiken schwierig
- ★ Stress (evtl. gezielt aufgebaut)
- ★ (anerzogene) Hilfsbereitschaft
- ★ Macht der Gewohnheit
- ★ Egoismus / Egozentrik bei jedem vorhanden

Aufgefallen im Gebäude, und dann?

- ★ Klassisches Social Engineering hilft weiter, wenn ein Angreifer „entdeckt“ wird
- ★ Selbst professionelle Mitarbeiter des Objektschutzes im Hochsicherheitsbereich verhalten sich bei gut gewählten Erklärungen falsch

Beispiel:

„Wir führen hier gerade eine Sicherheitsüberprüfung im Auftrag der Geschäftsleitung durch. Ich notiere Ihren Namen, damit ich sie lobend erwähnen kann. Bitte behalten sie über die Prüfung Stillschweigen, damit wir weiter testen können.“

Aufgefallen im Gebäude, und dann?

- ★ Klassisches Social Engineering hilft weiter, wenn ein Angreifer „entdeckt“ wird
- ★ Selbst professionelle Mitarbeiter des Objektschutzes im Hochsicherheitsbereich verhalten sich bei gut gewählten Erklärungen falsch

Beispiel:

„Wir führen hier gerade eine Sicherheitsüberprüfung im Auftrag der Geschäftsleitung durch. Ich notiere Ihren Namen, damit ich sie lobend erwähnen kann. Bitte behalten sie über die Prüfung Stillschweigen, damit wir weiter testen können.“

Mobile IT-Hardware: Laptops

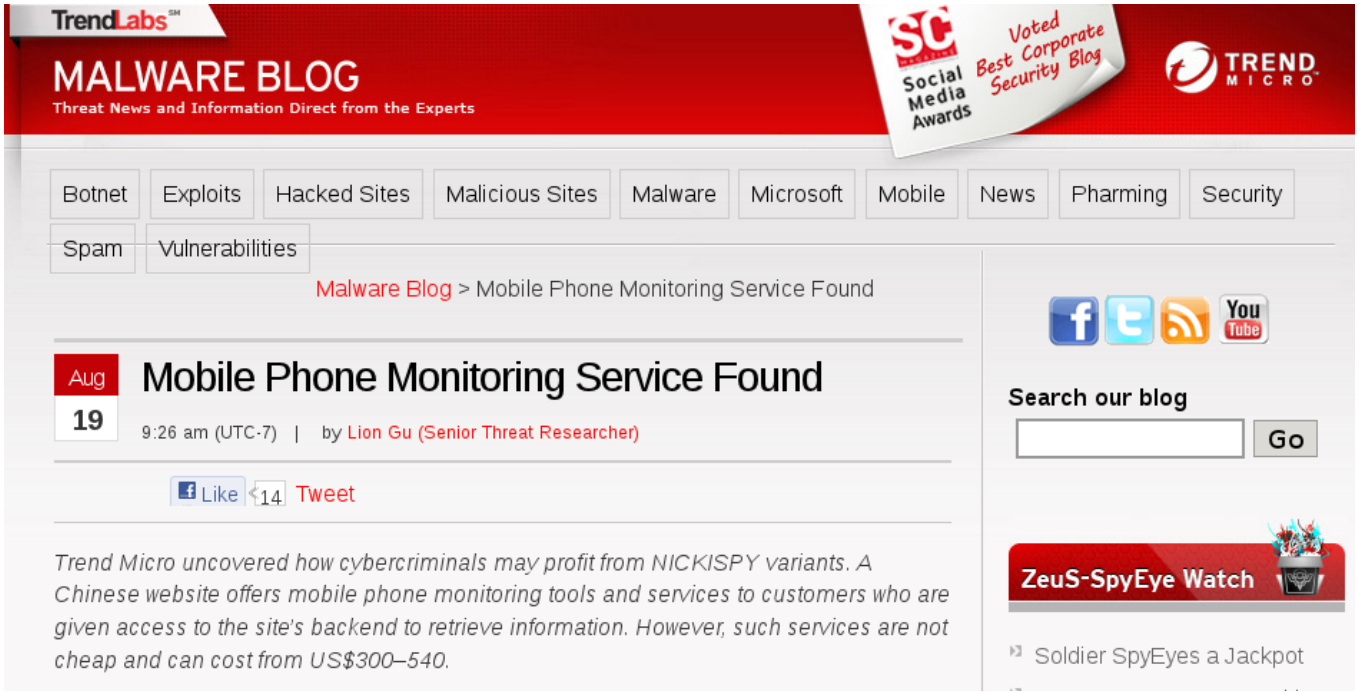
Problem: Ihre Mitarbeiter tragen ihre vertraulichen Daten bei Geschäftsreisen aus dem Unternehmen.

Mobile IT-Hardware: Laptops

Problem: Ihre Mitarbeiter tragen ihre vertraulichen Daten bei Geschäftsreisen aus dem Unternehmen.

Mobile IT-Hardware: Mobiltelefone

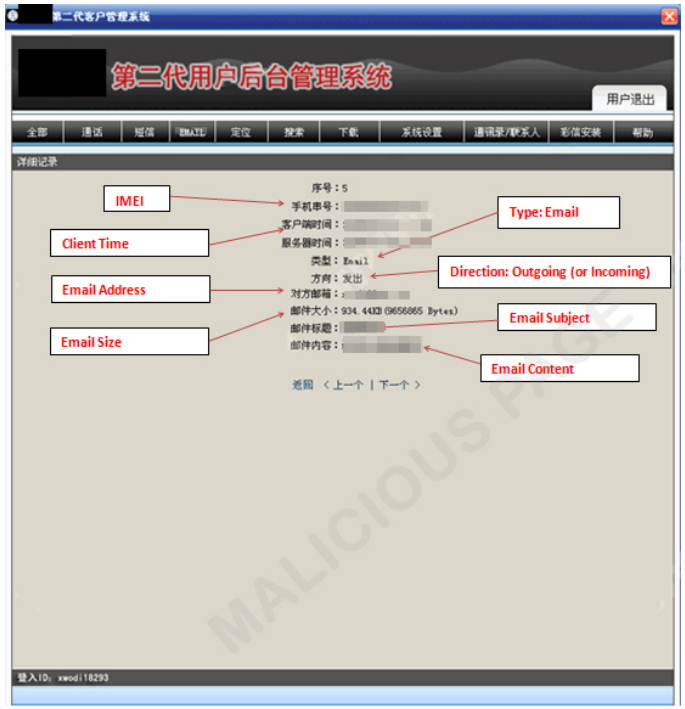
Servicelösung für Industriespione: Mobiltelefon-Monitoring



http://blog.trendmicro.com/mobile-phone-monitoring-service-found/

Mobile IT-Hardware: Mobiltelefone

Servicelösung für Industriespione: Mobiltelefon-Monitoring

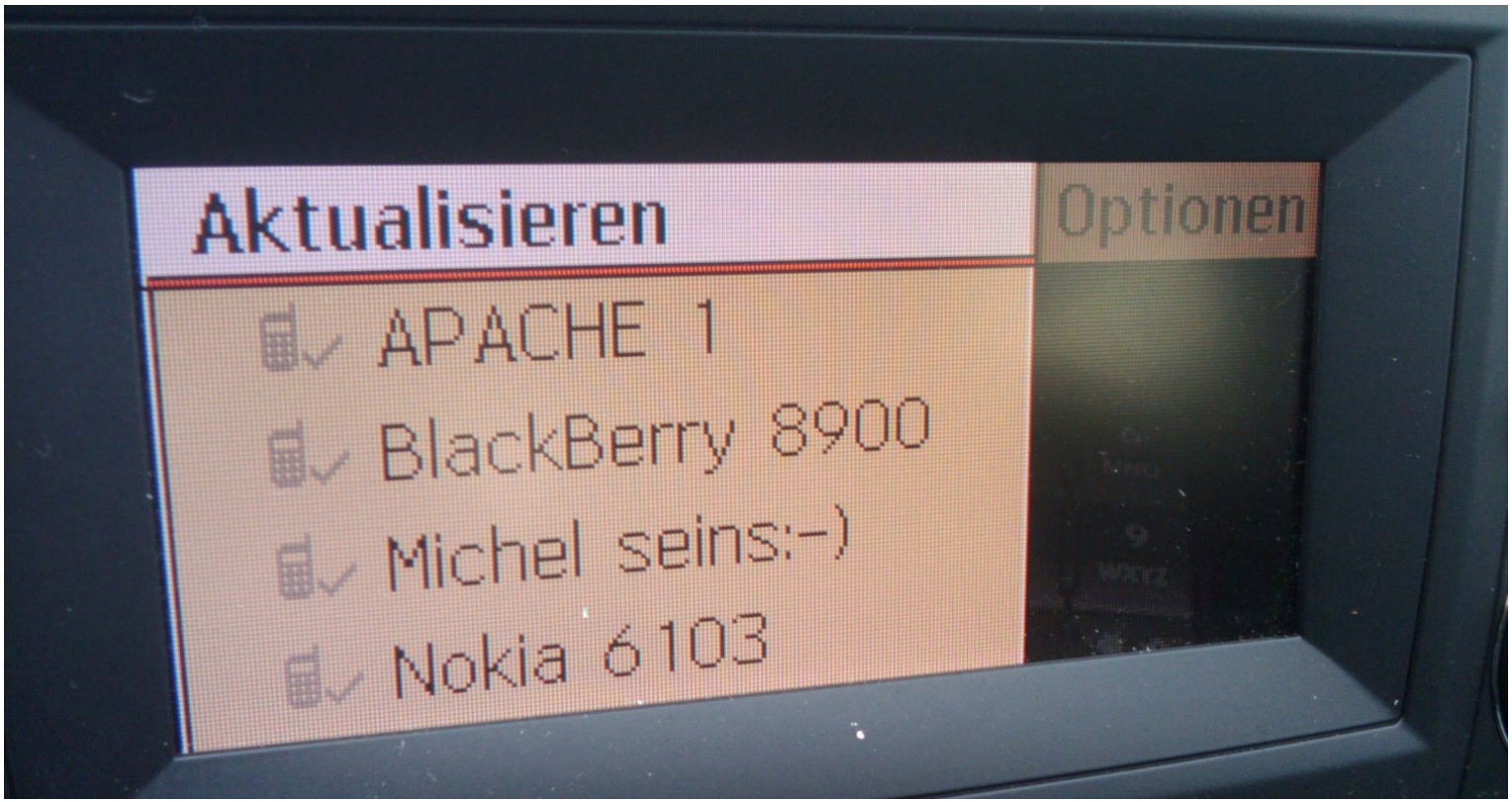


Bildquelle: http://blog.trendmicro.com/mobile-phone-monitoring-service-found/

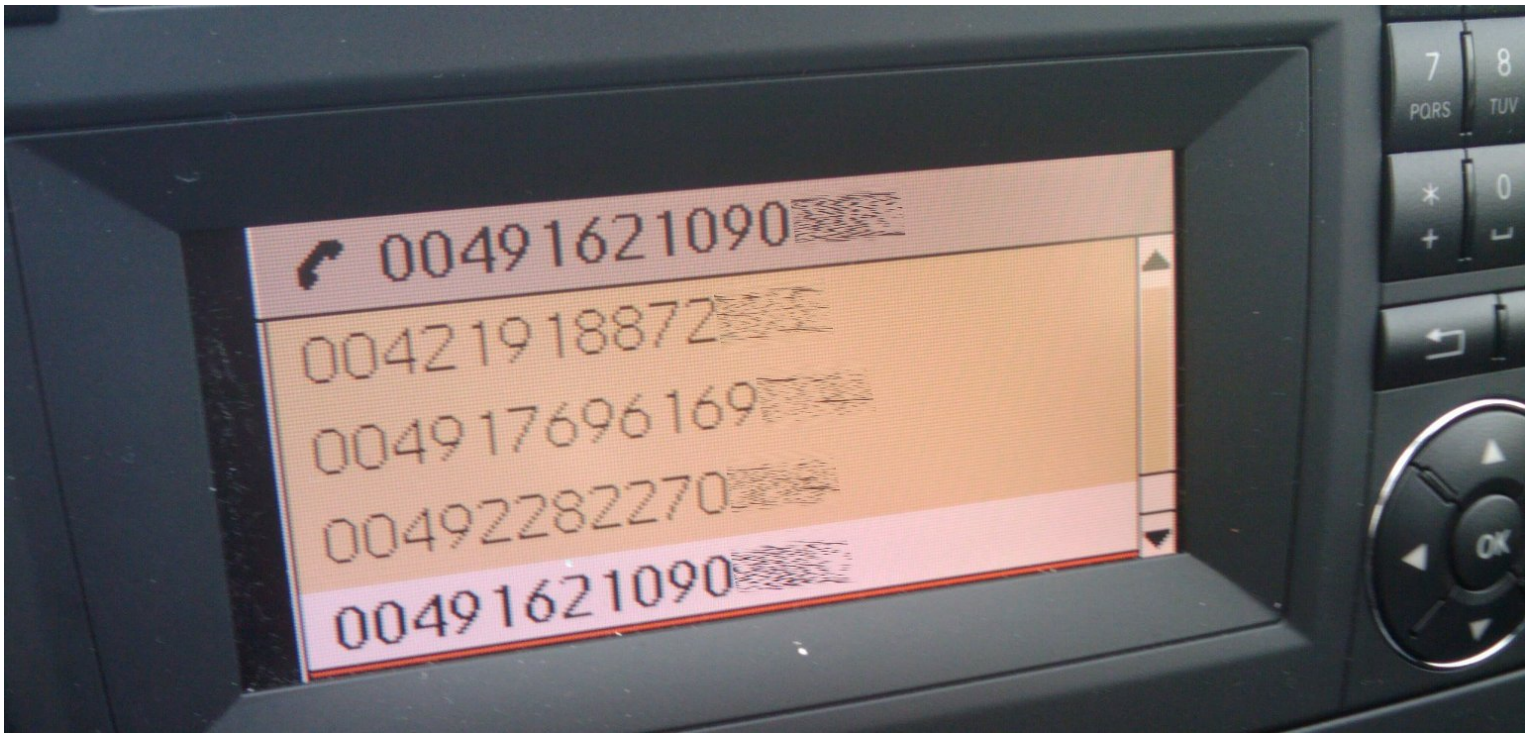
Mietwagen: Navigationsgeräte

Mietwagen: Telefone

Mietwagen: Telefone



Mietwagen: Telefone



Hotels

- ★ Auch im Hotelzimmer gilt: Wahlwiederholung beim Telefon beachten
- ★ Die meisten Hoteltüren sind nicht sicher abschließbar
- ★ Über Hotelsafes könnte man eigene Vorträge halten

⇒ Hotels sind kein guter Ort, um wichtige Daten zu lagern!

Hoteltüren

Hoteltüren

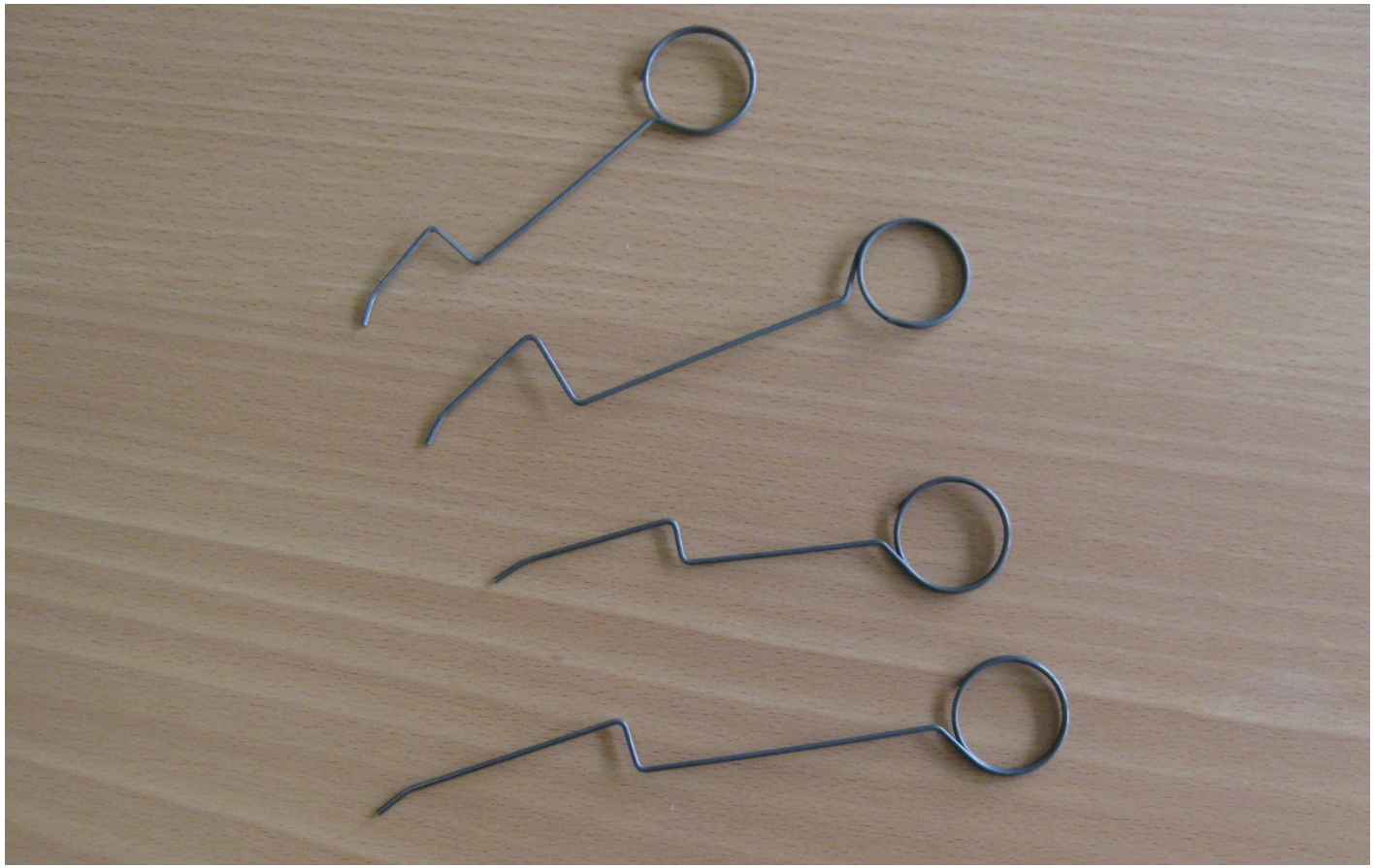
Was möchte ein Angreifer?

- ★ Diebstahl von Hardware (nicht IT-spezifisch)
- ★ Zugriff auf Daten (evtl. auch durch Diebstahl)
- ★ Datenmanipulation / Sabotage
- ★ Zugriff auf Netzwerk
- ★ Manifestierung im Netzwerk

Klassisches Lockpicking

Werkzeuge: Keilformgleiter

Werkzeuge: Türfallennadeln



Werkzeuge: Türklinkenangel

Der klassische Irrtum: Abgeschlossene Türen

„Meine Türen sind doch abgeschlossen!“

- ★ Grundsatz in Pentests: Alles hinterfragen
- ★ Viele „abgeschlossene“ Türen sind nicht abgeschlossen
- ★ „Aber *meine* Türen sind doch abgeschlossen...“
  ⇒ **Wetten, dass nicht?**

Der klassische Irrtum: Abgeschlossene Türen

„Meine Türen sind doch abgeschlossen!“

- ★ Grundsatz in Pentests: Alles hinterfragen
- ★ Viele „abgeschlossene“ Türen sind nicht abgeschlossen
- ★ „Aber *meine* Türen sind doch abgeschlossen...“
  ⇒ **Wetten, dass nicht?**

Eingangs- und Zwischentüren

- ★ Eingangstüren mit Summer
- ★ Zwischentüren mit Chipkarten/Fingerprint/Code sind meistens nicht abgeschlossen

Aus einem Penetrationstest

Glaszwischentüre, Chipkarten gesichert, von innen live videoüberwacht. Angriff mit Türfallennadeln: Kurzes Vortäuschen einer Chipkarte, dann Türöffnung in 1-2 Sekunden per Nadel. Auf dem Video ist der Angriff kaum zu erkennen.

Eingangs- und Zwischentüren

- ★ Eingangstüren mit Summer
- ★ Zwischentüren mit Chipkarten/Fingerprint/Code sind meistens nicht abgeschlossen

Aus einem Penetrationstest

Glaszwischentüre, Chipkarten gesichert, von innen live videoüberwacht. Angriff mit Türfallennadeln: Kurzes Vortäuschen einer Chipkarte, dann Türöffnung in 1-2 Sekunden per Nadel. Auf dem Video ist der Angriff kaum zu erkennen.

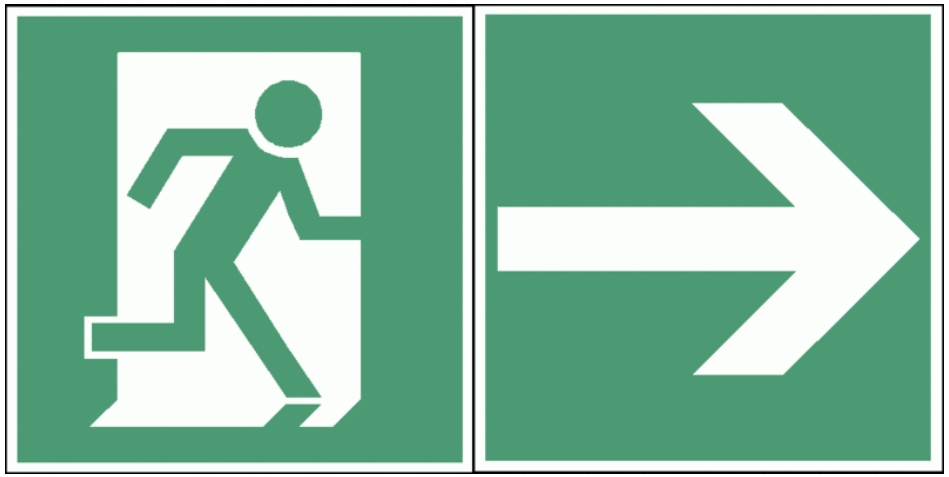
Eingangs- und Zwischentüren

- ★ Eingangstüren mit Summer
- ★ Zwischentüren mit Chipkarten/Fingerprint/Code sind meistens nicht abgeschlossen

Aus einem Penetrationstest

Glaszwischentüre, Chipkarten gesichert, von innen live videoüberwacht. Angriff mit Türfallennadeln: Kurzes Vortäuschen einer Chipkarte, dann Türöffnung in 1-2 Sekunden per Nadel. Auf dem Video ist der Angriff kaum zu erkennen.

Fluchtwege und Türen



Fluchttüren

Fluchttüren müssen, um Panikfallen zu vermeiden, einfach (mit einer Hand) in Fluchtrichtung zu öffnen sein.

Fluchtwege und Türen

- ★ Fluchttüren können durchaus abgeschlossen sein
- ★ Die einfache Betätigung der Türklinke oder z.B. einer Querstange zieht in diesem Fall auch den Riegel zurück.
- ★ Öffnung von außen: Meistens mit Hilfe der Türklinkenangel
- ★ Bei wenig Platz unterhalb der Türe: Türe z.B. mit pneumatischem Hebekisten leicht anheben.
- ★ Angreifer können Fluchtwegen „rückwärts“ folgen...

Fluchtwege und Türen

- ★ Fluchttüren können durchaus abgeschlossen sein
- ★ Die einfache Betätigung der Türklinke oder z.B. einer Querstange zieht in diesem Fall auch den Riegel zurück.
- ★ Öffnung von außen: Meistens mit Hilfe der Türklinkenangel
- ★ Bei wenig Platz unterhalb der Türe: Türe z.B. mit pneumatischem Hebekisten leicht anheben.
- ★ Angreifer können Fluchtwegen „rückwärts“ folgen...

Serverräume

- ★ Interessantes Ziel für Angreifer
- ★ In der Praxis: Lokalisierung für Angreifer meistens einfach
- ★ Oft mit Gaslöschanlagen ausgestattet
- ★ Gaslöschanlagen ⇒ Fluchttüren müssen vorhanden sein, da Personen bei Auslösung der Löschanlage den Raum verlassen müssen

Serverräume

- ★ Interessantes Ziel für Angreifer
- ★ In der Praxis: Lokalisierung für Angreifer meistens einfach
- ★ Oft mit Gaslöschanlagen ausgestattet
- ★ Gaslöschanlagen $\Rightarrow$ Fluchttüren müssen vorhanden sein, da Personen bei Auslösung der Löschanlage den Raum verlassen müssen

Datenvernichtung

- ★ Eine richtige (und konsequente) Datenvernichtung ist wichtig
- ★ Im digitalen Bereich: Festplatteninhalte sicher löschen (überschreiben)
- ★ Im analogen Bereich: Shredder/Aktenvernichter

Beispiel Lebenszyklus vertraulicher Papierdaten

Ein Kunde stellt folgendem Ablauf dar:

- ★ Morgens erhält Callcenter-Mitarbeiter Papierliste
- ★ Einträge werden abgehakt
- ★ Notizen während der Telefonate auf extra Papier notiert
- ★ Einträge und Notizen werden in EDV übertragen
- ★ Abends wird Liste in spezielle Ablage gelegt
- ★ Notizen kommen in Papiermüll
- ★ Ablage wird abends geleert und sicher verwahrt
- ★ Mülleimerinhalt wird abends per Shredder vernichtet

Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen

Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen

Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum

Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer

Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer
- ★ Mülleimer ist nicht geleert, es finden sich Listen mit Notizen

Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer
- ★ Mülleimer ist nicht geleert, es finden sich Listen mit Notizen
- ★ Weitere Listen finden sich (einmal zerissen) im Papiermüll auf dem Firmengelände. Zugriff für jedermann ist möglich.

Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer
- ★ Mülleimer ist nicht geleert, es finden sich Listen mit Notizen
- ★ Weitere Listen finden sich (einmal zerissen) im Papiermüll auf dem Firmengelände. Zugriff für jedermann ist möglich.
- ★ Rekonstruktion von fast 100% der Listen der vergangenen Tage gelingt

Beispiel Lebenszyklus vertraulicher Papierdaten

Es zeigte sich:

- ★ Notizen finden sich nicht auf extra Papier, sondern auf Listen
- ★ Notizen und Listen werden nicht täglich in EDV übertragen
- ★ Listen mit Notizen finden sich überall im Raum
- ★ Die für die Listen vorgesehene Ablage ist leer
- ★ Mülleimer ist nicht geleert, es finden sich Listen mit Notizen
- ★ Weitere Listen finden sich (einmal zerissen) im Papiermüll auf dem Firmengelände. Zugriff für jedermann ist möglich.
- ★ Rekonstruktion von fast 100% der Listen der vergangenen Tage gelingt
- ★ Es existiert firmenweit überhaupt kein Shredder!

Empfehlungen Datenvernichtung

- ★ Nutzen Sie Shredder (mindenstens Sicherheitsstufe 4)!
- ★ Prüfen Sie regelmäßig, ob Ihre Mitarbeiter die Aktenvernichter auch nutzen (der Mülleimer ist bequemer!).
- ★ Überprüfen Sie regelmäßig, ob der Shredder auch wirklich (noch) korrekt arbeitet
- ★ Bei externen Datenvernichtungsunternehmen: Was ist mit der Datensicherheit bis zur Vernichtung?

Fazit

- ★ Industriespionage findet statt

Fazit

- ★ Industriespionage findet statt
- ★ Sind Ihre Türen abgeschlossen?

Fazit

- ★ Industriespionage findet statt
- ★ Sind Ihre Türen abgeschlossen?
- ★ Wie wird bei Ihnen auf betriebsfremde Personen reagiert?

Fazit

- ★ Industriespionage findet statt
- ★ Sind Ihre Türen abgeschlossen?
- ★ Wie wird bei Ihnen auf betriebsfremde Personen reagiert?
- ★ Schulen Sie Ihre Mitarbeiter!

Fazit

- ★ Industriespionage findet statt
- ★ Sind Ihre Türen abgeschlossen?
- ★ Wie wird bei Ihnen auf betriebsfremde Personen reagiert?
- ★ Schulen Sie Ihre Mitarbeiter!
- ★ Erkennen Sie Ihre 10% der wirklich wichtigen Daten...

Fazit

- ★ Industriespionage findet statt
- ★ Sind Ihre Türen abgeschlossen?
- ★ Wie wird bei Ihnen auf betriebsfremde Personen reagiert?
- ★ Schulen Sie Ihre Mitarbeiter!
- ★ Erkennen Sie Ihre 10% der wirklich wichtigen Daten...
- ★ ...und schützen Sie diese adäquat!

Fragen?

Vielen Dank für Ihre Aufmerksamkeit