Sicherheit und Industriespionage – Von technischen und menschlichen Schwächen

Patrick Hof - RedTeam Pentesting GmbH
patrick.hof@redteam-pentesting.de
http://www.redteam-pentesting.de

ESMT Netzwerk-Tag 2011
22. November 2011, Schloss Gracht

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!

Was möchte ein Angreifer?

Konkurrenzausspähung (Industriespionage)

Ausforschung ausgehend von Mitbewerbern.

- ★ Zugriff auf Netzwerk
- ★ Manifestierung im Netzwerk
- ★ Zugriff auf Daten (eventuell auch durch Diebstahl)
- ★ Datenmanipulation / Sabotage

Wie kommt ein Angreifer an unsere Daten?

- ★ Sicherheit muss ein Gesamtkonzept sein, denn ein Angreifer sucht sich die schwächste Stelle
- ★ Im Folgenden: Häufige/Interessante Schwachstellen aus verschiedenen Bereichen

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

Mobile IT-Hardware: Laptops

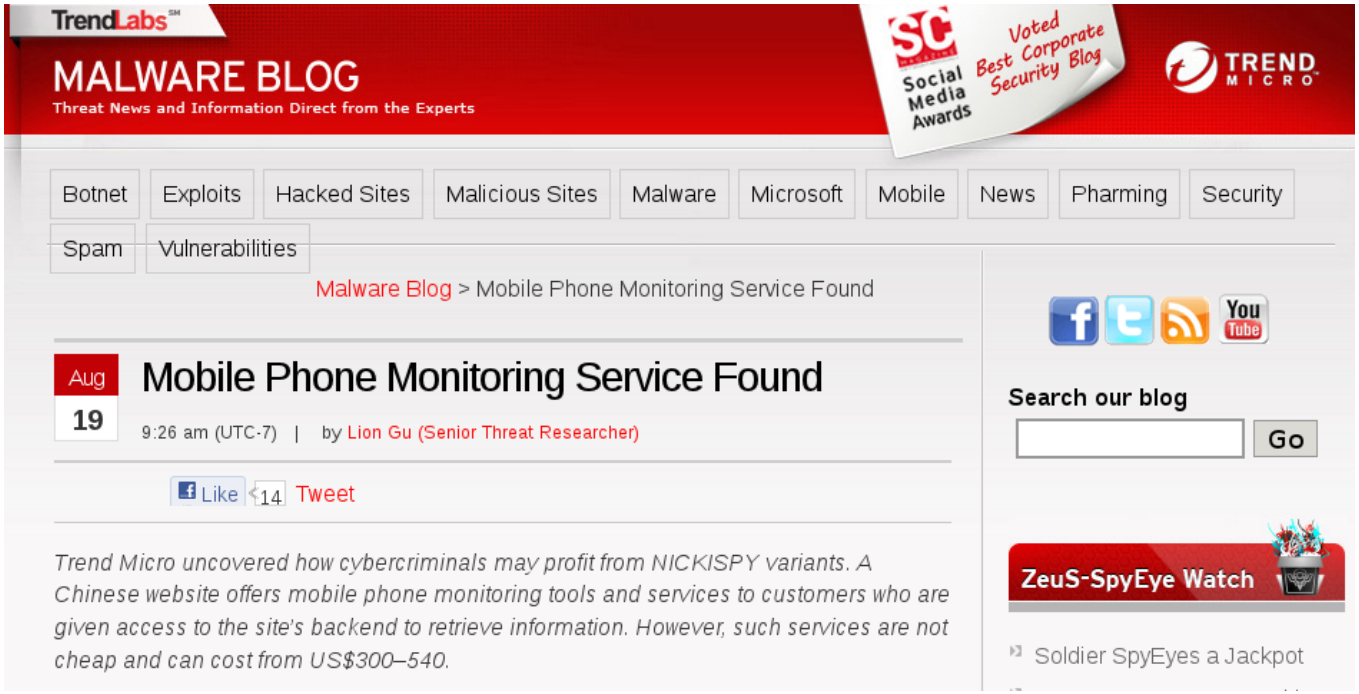
Problem: Ihre Mitarbeiter tragen ihre vertraulichen Daten bei Geschäftsreisen aus dem Unternehmen.

Mobile IT-Hardware: Laptops

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

Mobile IT-Hardware: Mobiltelefone

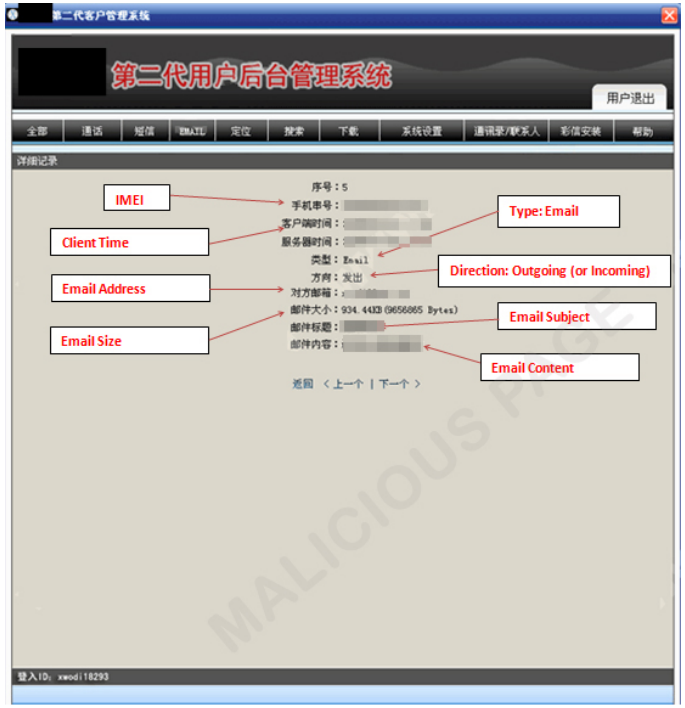
Servicelösung für Industriespione: Mobiltelefon-Monitoring



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

Mobile IT-Hardware: Mobiltelefone

Servicelösung für Industriespione: Mobiltelefon-Monitoring

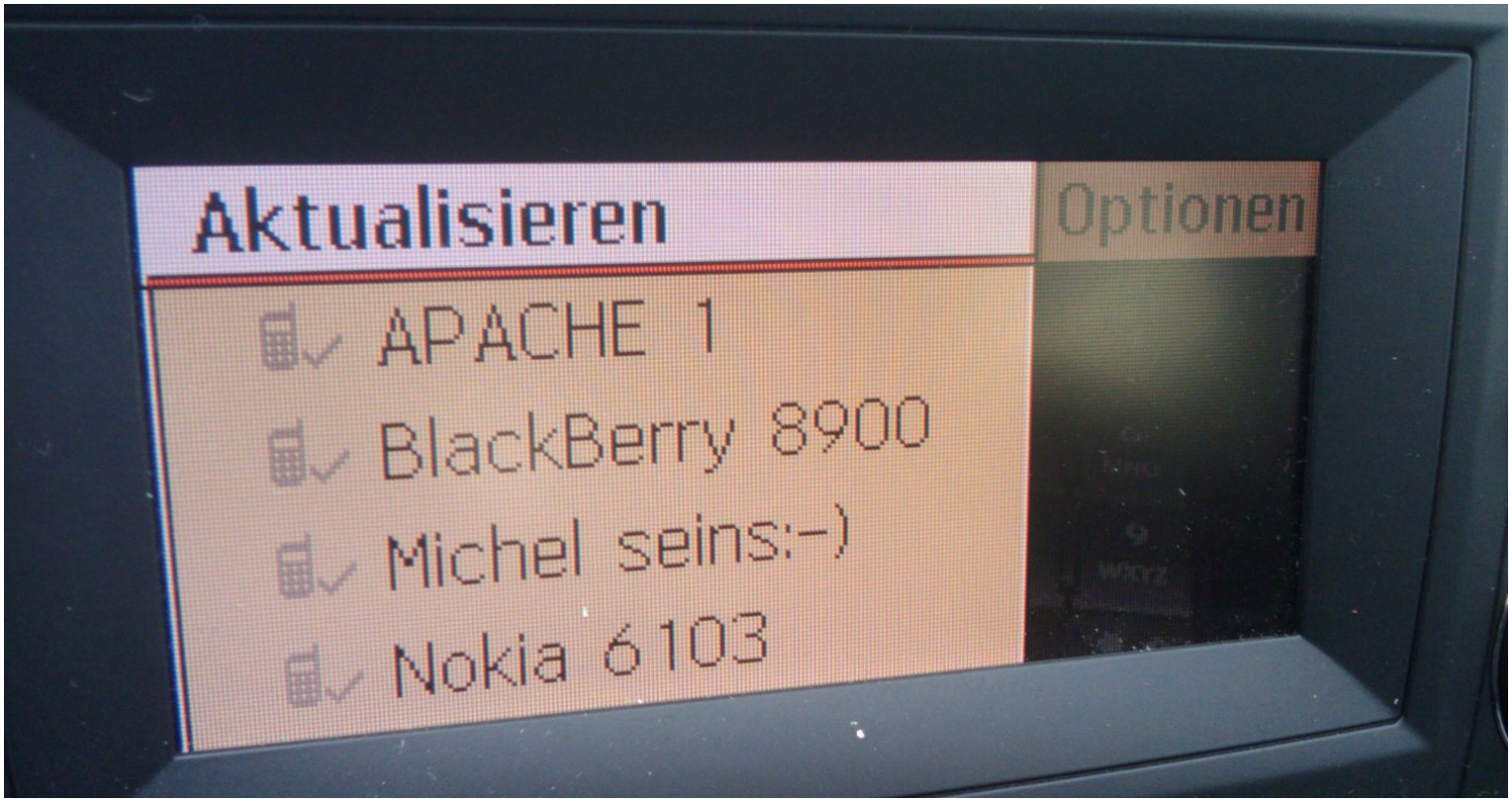


Bildquelle: http://blog.trendmicro.com/mobile-phone-monitoring-service-found/

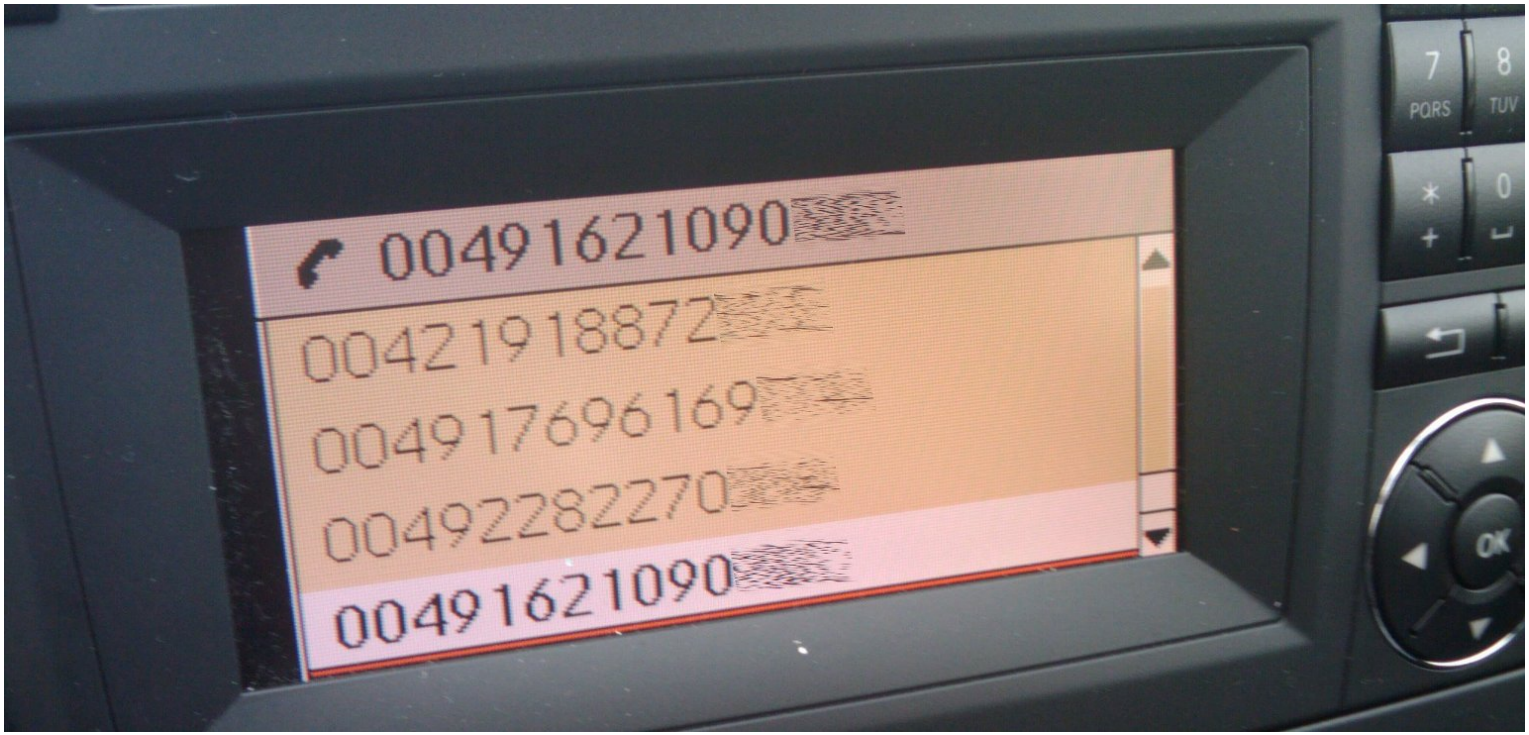
Mietwagen: Navigationsgeräte

Mietwagen: Telefone

Mietwagen: Telefone



Mietwagen: Telefone



Hotels

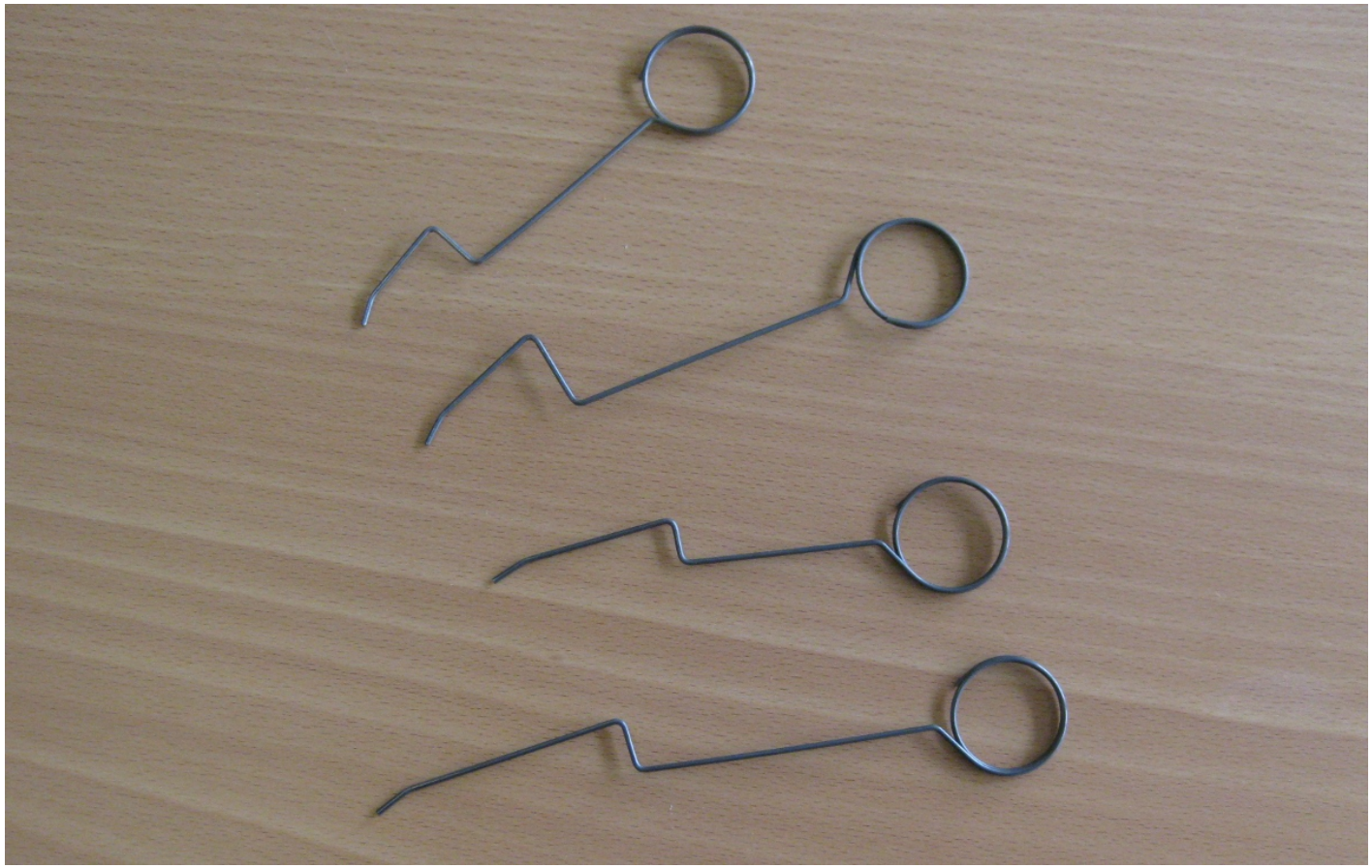
- ★ Auch im Hotelzimmer gilt: Wahlwiederholung beim Telefon beachten
- ★ Die meisten Hoteltüren sind nicht sicher abschließbar
- ★ Über Hotelsafes könnte man eigene Vorträge halten

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

Klassisches Lockpicking

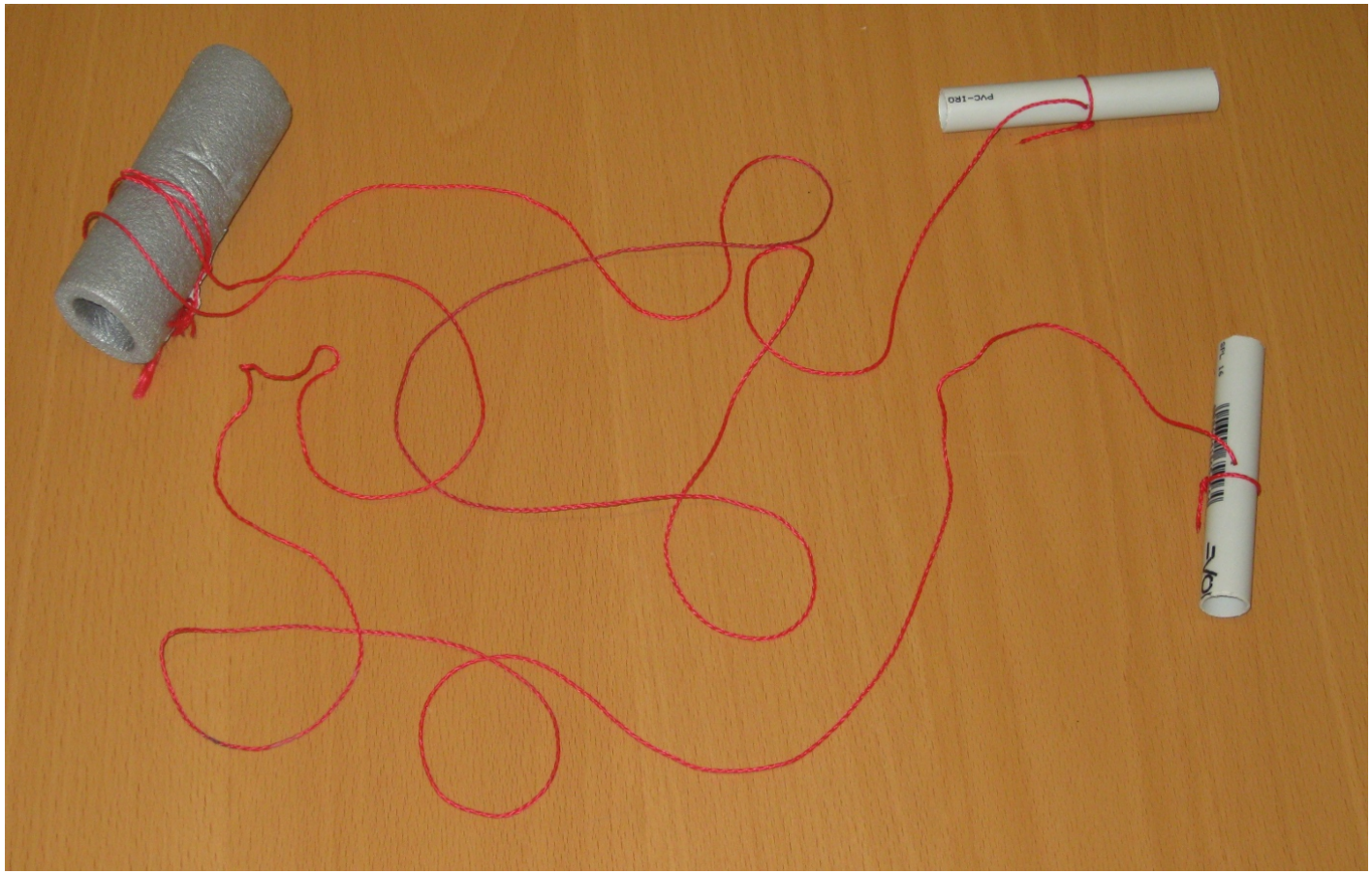
Werkzeuge: Keilformgleiter

Werkzeuge: Türfallennadeln



Werkzeuge: Türklinkenangel

Werkzeuge: Kippfenster/-Türöffnung



Hoteltüren

Manchmal funktioniert es sogar noch einfacher:

Hoteltüren

Manchmal funktioniert es sogar noch einfacher:

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

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

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

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

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

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

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

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

Penetrationstest deckt nachts auf:

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

Beispiel Lebenszyklus vertraulicher Papierdaten

Penetrationstest deckt nachts auf:

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

Beispiel Lebenszyklus vertraulicher Papierdaten

Penetrationstest deckt nachts auf:

- ★ 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

Penetrationstest deckt nachts auf:

- ★ 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

Penetrationstest deckt nachts auf:

- ★ 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

Penetrationstest deckt nachts auf:

- ★ 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

Penetrationstest deckt nachts auf:

- ★ 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

Penetrationstest deckt nachts auf:

- ★ 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!

Fazit 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?

Weitere Denkanstöße

- ★ Fremde Hardware an eigenem Rechner (USB-Sticks, Firewire, etc.)
- ★ Funkverbindungen (WLAN, Bluetooth, Funktastaturen, RFID, etc.), Clients beachten!
- ★ Besondere Situationen (z.B. Einreise USA, UK)

Fazit

- ★ Industriespionage findet statt

Fazit

- ★ Industriespionage findet statt
- ★ Auch bei Ihnen!

Fazit

- ★ Industriespionage findet statt
- ★ Auch bei Ihnen!
- ★ Schützen Sie sich durch ein ganzheitliches Sicherheitskonzept

Fragen?

Vielen Dank für Ihre Aufmerksamkeit