Sicherheit und Industriespionage: Ein Realitätsabgleich

Von falschen Sicherheitsversprechen, überraschenden Risiken und Insellösungen

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

Praktische IT-Sicherheit
31. August 2010, Hochschule Bonn-Rhein-Sieg

RedTeam Pentesting, Daten & Fakten

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

Wirtschafts- und Industriespionage

Wirtschaftsspionage

Ausforschung ausgehend/unterstützt von ausländischen staatlichen Stellen (Nachrichtendienste).

Konkurrenzausspähung (Industriespionage)

Ausforschung ausgehend von Mitbewerbern.

Zusammenhang Penetrationstests und Industriespionage

- ★ Kunden berichten regelmäßig über Fälle von Industriespionage
- ★ Größenordnung: Kunden mit ca. 10 Mitarbeitern bis zu Angreifern mit geschätztem Budget von ca. 10 Millionen Euro
- ★ Penetrationstests als schnelle Maßnahme zum Aufdecken von Schwachstellen noch während andauernder Angriffe
- ★ $\Rightarrow$ Viele Informationen aus erster Hand

Zusammenhang Penetrationstests und Industriespionage

- ★ Kunden berichten regelmäßig über Fälle von Industriespionage
- ★ Größenordnung: Kunden mit ca. 10 Mitarbeitern bis zu Angreifern mit geschätztem Budget von ca. 10 Millionen Euro
- ★ Penetrationstests als schnelle Maßnahme zum Aufdecken von Schwachstellen noch während andauernder Angriffe
- ★ $\Rightarrow$ Viele Informationen aus erster Hand

Beispiele von Industriespionage

Beispiel 1

Kunde berichtet: Mehrjährige nicht-öffentliche Entwicklung eines Produktes aus dem Bereich des Maschinenbaus steht vor dem Abschluss. Noch bevor das Produkt der Öffentlichkeit vorgestellt wird, stellt ein chinesischer Anbieter ein offensichtlich baugleiches Produkt auf einer deutschen Fachmesse aus.

Analyse: Beispiel 1

- ★ Vermutung: Chinesischer Anbieter hatte jederzeit Zugriff auf Baupläne
- ★ Ablauf des Informationsabflusses konnte nicht geklärt werden
- ★ Wirtschaftliche Folgen noch nicht abschätzbar

Beispiele von Industriespionage

Beispiel 2

Firma X (ca. 20 Mitarbeiter) stellt massive Einbrüche bei Vertragsabschlüssen fest. Einzelne Kunden erwähnen, dass sich ein Mitbewerber mit ähnlichem Produkt unaufgefordert kurz vor dem Termin mit X meldete.

Rücksprache mit allen potentiellen Neukunden ergibt, dass der Mitbewerber überall jeweils nur Tage vor dem Termin mit X selber vorstellig wurde.

Analyse: Beispiel 2

- ★ Mitbewerber hatte Zugriff auf CRM-System mit Kundenterminen
- ★ Zugriff mit großer Wahrscheinlichkeit über eine Schwachstelle im Internetauftritt von X
- ★ Hinweise in den Logdateien deuten auf deutsche Firma aus dem Umfeld des Mitbewerbers
- ★ Leider sind Logdaten nicht gerichtsfest
- ★ Gerichtliche Verfolgung findet nicht statt, obwohl Mitbewerber als auch potentielle Angreifer-IP aus Deutschland stammen
- ★ Folgen ebben nach Korrektur der Schwachstelle schnell ab, Firma X überlebt

Fazit Industriespionage

- ★ 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: Häufige/Interessante Schwachstellen aus verschiedenen Bereichen

Definition: Physische Sicherheit

Physical Security

Physical security describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media.

(Wikipedia)

Technische Zugangskontrollsysteme

Technische Zugangskontrollsysteme

Definition Biometrie

Biometrie

[. . .] Heute definiert man Biometrie im Bereich der Personenerkennung auch als automatisierte Erkennung von Individuen, basierend auf ihren Verhaltens- und biologischen Charakteristika.

(Wikipedia)

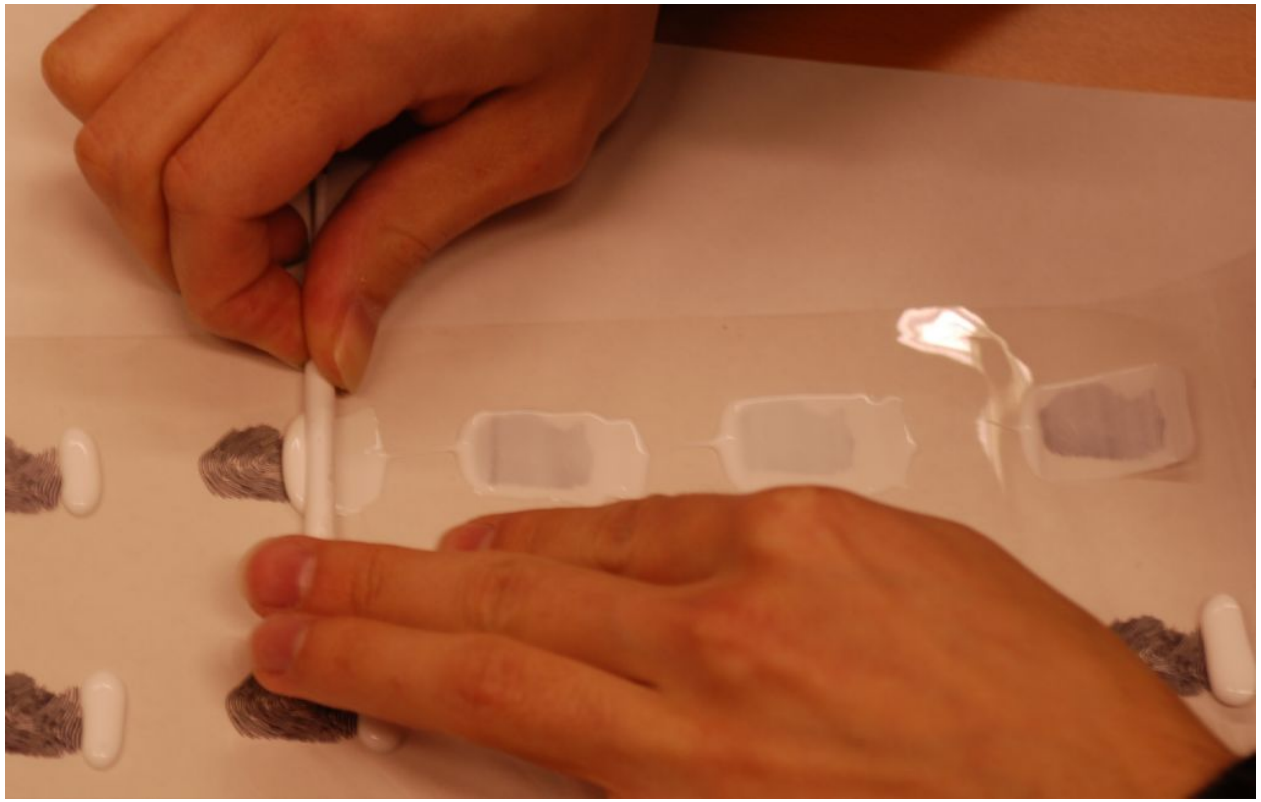
Fingerabdrücke: Einige Herstelleraussagen...

Fingerabdrücke sind individuell und nicht kopierbar.

Fingerabdrücke sind praktisch, modern und absolut sicher.

Es ist so gut wie unmöglich die biometrischen Merkmale zu stehlen oder zu fälschen.

Replizieren von Fingerabdrücken



Replizieren von Fingerabdrücken

Risiken bei Biometrie: Was zu beachten ist

- ★ Abwägung zwischen Bequemlichkeit und Sicherheit
- ★ Kann das genutzte Merkmal erfolgreich kopiert werden, so steht oft kein neues (anderes) zur Verfügung
- ★ Biometrie kann Seiteneffekte haben (z.B. körperliche Unversehrtheit, Zugangskontrolle BND Berlin)
- ★ Große Unterschiede zwischen Theorie und Praxis
  $\Rightarrow$ Verlassen Sie sich nicht auf Werbeaussagen!

„Harmlose“ Telefone

- In Zusammenhang mit Industriespionage wird gerne an Manipulationen von Telefonen gedacht („Wanzen“)
- Oft ist es in der Praxis aber viel einfacher...

DECT-Sicherheit

- ★ DECT-Telefone sind weit verbreitet
- ★ Abhören in der Praxis trivial (Hardwarekosten 20 Euro)
- ★ `http://www.dedected.org`

DECT-Sicherheit

- ★ DECT-Telefone sind weit verbreitet
- ★ Abhören in der Praxis trivial (Hardwarekosten 20 Euro)
- ★ `http://www.dedected.org`

DECT Sicherheit

DECT FORUM Statement:

The DECT Forum also states that it is a criminal act to eavesdrop telephone conversations. It is impossible to accidentally eavesdrop on telephone conversations and therefore the risk for users is very low. Only those with a clear criminal energy and intent and a sophisticated knowledge would be capable of eavesdropping.

(DECT Forum: http://www.dect.org/news.aspx?id=41)

GSM-Sicherheit

- GSM-Handy-Verschlüsselung (A5/1) kann gebrochen werden
- Hardwarekosten zum Mitschneiden: ca. 1500 US-Dollar
- Karsten Nohl: „Das Mitschneiden und Knacken von GSM ist heute so einfach wie Angriffe auf WLAN vor einigen Jahren.“
- `http://reflextor.com/trac/a51`

GSM-Sicherheit

GSM Association Statement:

The theoretical compromise [...] requires the construction of a large look-up table of approximately 2 Terabytes - this is equivalent to the amount of data contained in a 20 kilometre high pile of books [...] In theory, someone with access to the data in such a table could use it to analyse an encrypted call and recover the encryption key.

(The Register: `http://www.theregister.co.uk/2009/08/28/mobile_phone_snooping_plan/`)

Voice over IP

- ★ Viele Firmen setzen bereits VoIP ein
- ★ Die anderen migrieren gerade

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

„Push Audio“

- ★ Senden von Audio-Daten an die Endgeräte, welche automatisch abgespielt werden

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

„Push Audio“

- Senden von Audio-Daten an die Endgeräte, welche automatisch abgespielt werden
- z.B. Feueralarm...

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Fernsteuerung der Bedienelemente

- ★ Umleiten von Telefonaten
- ★ Abhören per Konferenzschaltung

 Jean-Etienne Poirrier

Voice over IP: Neue Features, neue Risiken

VoIP-Geräte haben neue Funktionalitäten – und Risiken:

Gute Mikrofone

- ★ Einschalten der Freisprecheinrichtung
- ★ ⇒ Raumüberwachung per Telefon

 Jean-Etienne Poirrier

Voice over IP: Zusammenfassung

- ★ Fehler herstellerübergreifend
- ★ Auch physische Trennung der Netzwerke hilft oft nicht
- ★ Fehler sind teilweise auch auf Nicht-VoIP-Telefone übertragbar

 Jean-Etienne Poirrier

Datenvernichtung

- ★ Eine richtige (und konsequente) Datenvernichtung ist wichtig
- ★ Im digitalen Bereich: Festplatteninhalte sicher löschen (mehrfach 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!).
- ★ 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)
- ★ Physische Sicherheit

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