



Physical Security

—

Wenn Türen zu Firewalls werden

Jens Liebchen (jens.liebchen@redteam-pentesting.de)

RedTeam Pentesting GmbH

<http://www.redteam-pentesting.de>

Lehrstuhl für IT-Sicherheitsinfrastrukturen

Universität Erlangen-Nürnberg

8. November 2011, Erlangen



Einführung

Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Wer wir sind

Warum Physical Security?
Penetrationstests und Physical Security

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Firmensitz in Aachen, weltweite Durchführung von Penetrationstests
- ★ Forschung im IT-Sicherheitsbereich





Einführung

Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Wer wir sind

Warum Physical Security?

Penetrationstests und Physical Security

Warum Physical Security?

- ★ Physical Security muss Teil der IT-Sicherheits-Strategie sein
- ★ Risiken kann nur begegnet werden, wenn diese auch bekannt sind
- ★ ⇒ **Awareness**





Warum Physical Security?

- ★ Physical Security muss Teil der IT-Sicherheits-Strategie sein
- ★ Risiken kann nur begegnet werden, wenn diese auch bekannt sind
- ★ ⇒ **Awareness**
- ★ Sie sparen mindestens 100 Euro für den Schlüsseldienst, wenn Sie Ihren Schlüssel beim nächsten Mal drinnen liegen lassen :-)





Penetrationstests und Physical Security

Penetrationstests

Penetrationstests sind individuelle realitätsnahe Angriffe auf Netzwerke und Produkte im Auftrag des Eigentümers.

- ★ Security-Audits/Checklisten sind im Allgemeinen keine Penetrationstests
- ★ „Testen sie mal unsere Firewall...“ meistens auch nicht
- ★ Stattdessen: Was macht ein Angreifer in der Praxis?



Penetrationstests und Physical Security

Penetrationstests

Penetrationstests sind individuelle realitätsnahe Angriffe auf Netzwerke und Produkte im Auftrag des Eigentümers.

- ★ Security-Audits/Checklisten sind im Allgemeinen keine Penetrationstests
- ★ „Testen sie mal unsere Firewall...“ meistens auch nicht
- ★ Stattdessen: Was macht ein Angreifer in der Praxis?

Penetrationstests testen hauptsächlich Angriffe direkt auf die IT, in letzter Zeit wird aber immer mehr auch die physische Sicherheit in die Tests integriert.



Beschaffung von Werkzeugen/Rechtliches

- ★ Baumarkt!
- ★ Großhandel/Fachhändler für Schlüsseldienste
- ★ Normale Werkzeuge sind im Allgemeinen bezahlbar
- ★ Werkzeuge sind frei verkäuflich
- ★ Transport z.B. im Flugzeug ist unproblematisch
- ★ Vorsicht beim Üben an wichtigen Türen ⇒ Spuren und Problematik der Unterscheidung von echten Einbrüchen



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Beschaffung/Rechtliches
Werkzeuge für Türen
Werkzeuge für Kippfenster/-Türen

Klassisches Lockpicking





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Beschaffung/Rechtliches
Werkzeuge für Türen
Werkzeuge für Kippfenster/-Türen

Werkzeuge: Keilformgleiter





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Beschaffung/Rechtliches
Werkzeuge für Türen
Werkzeuge für Kippfenster/-Türen

Werkzeuge: Türfallennadeln





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Beschaffung/Rechtliches
Werkzeuge für Türen
Werkzeuge für Kipfenster/-Türen

Werkzeuge: Türklinkenangel

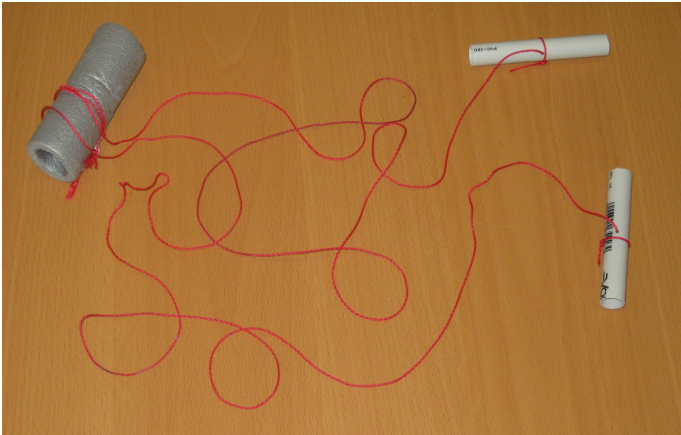




Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Beschaffung/Rechtliches
Werkzeuge für Türen
Werkzeuge für Kippfenster/-Türen

Werkzeuge: Kippfenster/-Türöffnung





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Was möchte ein Angreifer?

- ★ Diebstahl von Hardware (nicht IT-spezifisch)



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Was möchte ein Angreifer?

- ★ Diebstahl von Hardware (nicht IT-spezifisch)
- ★ Zugriff auf Daten (evtl. auch durch Diebstahl)



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Was möchte ein Angreifer?

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



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Was möchte ein Angreifer?

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



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



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Der klassische Irrtum: Abgeschlossene Türen

„Meine Türen sind doch abgeschlossen!“

- ★ Grundsatz in Pentests: Alles hinterfragen
- ★ Viele „abgeschlossene“ Türen sind nicht abgeschlossen



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?**



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Eingangs- und Zwischentüren

- ★ Eingangstüren mit Summer



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Eingangs- und Zwischentüren

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



Eingangs- und Zwischentüren

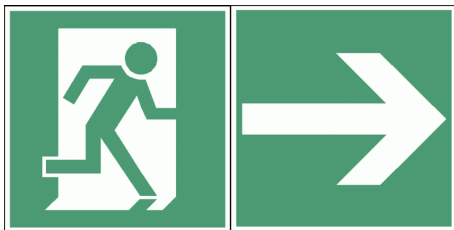
- ★ Eingangstüren mit Summer
- ★ Zwischentüren mit Chipkarten/Fingerprint/Code sind meistens nicht abgeschlossen

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.



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

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.



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...



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Serverräume

- ★ Interessantes Ziel für Angreifer
- ★ In der Praxis: Lokalisierung für Angreifer meistens einfach



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

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



Gekippte Fenster == Offene Fenster

Wenn die Fenster nicht alarmgesichert sind, existieren in großen Gebäuden immer Fenster, die nachts offen bleiben. Wie kommt der Angreifer an Fenster in oberen Etagen?

- ★ Leiter (trivial, wird aber häufig übersehen)
- ★ Abseilen von oben



Gekippte Fenster == Offene Fenster

Wenn die Fenster nicht alarmgesichert sind, existieren in großen Gebäuden immer Fenster, die nachts offen bleiben. Wie kommt der Angreifer an Fenster in oberen Etagen?

- ★ Leiter (trivial, wird aber häufig übersehen)
- ★ Abseilen von oben

Zitat aus einem Penetrationstest:

„Haben sie bedacht, dass ein Angreifer sich hier evtl. abseilt?“ —
„Das hatten wir schon...“ (und zwar nicht im Rahmen eines Penetrationstests)



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Mobile IT-Hardware

Der Angreifer ist nicht auf Ihr Gebäude beschränkt. Ihre Nutzer tragen die Daten aus dem Unternehmen.





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Mobile IT-Hardware

Der Angreifer ist nicht auf Ihr Gebäude beschränkt. Ihre Nutzer tragen die Daten aus dem Unternehmen.





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Hoteltüren

- ★ Die meisten Hoteltüren sind nicht sicher abschließbar
- ★ Zutritt mit den vorgestellten Werkzeugen ist fast immer möglich





Hoteltüren

- ★ Die meisten Hoteltüren sind nicht sicher abschließbar
- ★ Zutritt mit den vorgestellten Werkzeugen ist fast immer möglich
- ★ Über Hotelsafes könnte man eigene Vorträge halten





Hoteltüren

- ★ Die meisten Hoteltüren sind nicht sicher abschließbar
- ★ Zutritt mit den vorgestellten Werkzeugen ist fast immer möglich
- ★ Über Hotelsafes könnte man eigene Vorträge halten
- ★ ⇒ Hotels sind kein guter Ort, um wichtige Daten zu lagern!





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffsziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Hoteltüren

Manchmal funktioniert es sogar noch einfacher:





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Angriffziele
Abgeschlossene Türen
Gekippte Fenster
Mobilität und Reisen

Hoteltüren

Manchmal funktioniert es sogar noch einfacher:





Allgemein

- ★ Rein kommt ein Angreifer fast immer, ohne etwas zu beschädigen
- ★ Das Entdeckungsrisiko ist zumindest in großen Gebäuden gering
- ★ Personen in Gebäuden werden nur sehr selten hinterfragt



Allgemein

- ★ Rein kommt ein Angreifer fast immer, ohne etwas zu beschädigen
- ★ Das Entdeckungsrisiko ist zumindest in großen Gebäuden gering
- ★ Personen in Gebäuden werden nur sehr selten hinterfragt
- ★ Passwörter „hacken“ geht auch per Teleobjektiv (Passwörter werden immer noch aufgeschrieben)



Allgemein

- ★ Rein kommt ein Angreifer fast immer, ohne etwas zu beschädigen
- ★ Das Entdeckungsrisiko ist zumindest in großen Gebäuden gering
- ★ Personen in Gebäuden werden nur sehr selten hinterfragt
- ★ Passwörter „hacken“ geht auch per Teleobjektiv (Passwörter werden immer noch aufgeschrieben)
- ★ Die gefühlte Aufregung ist selbst während eines Penetrationstests relativ hoch



Beispiel: Netzwerkzugriff

- ★ In fast allen Räumen finden sich gepatchte Netzwerkdosen
- ★ Oft reicht das Überwinden einer einzigen Türe, um Zugriff auf das interne Netzwerk zu erhalten
- ★ Bodentanks öffnen: Es finden sich häufig Netzwerkdosen, die den Verantwortlichen nicht bewusst sind



Beispiel: Netzwerkzugriff

- ★ In fast allen Räumen finden sich gepatchte Netzwerkdosen
- ★ Oft reicht das Überwinden einer einzigen Türe, um Zugriff auf das interne Netzwerk zu erhalten
- ★ Bodentanks öffnen: Es finden sich häufig Netzwerkdosen, die den Verantwortlichen nicht bewusst sind
- ★ VoIP-Netzwerke
 - ★ Zugriff in einem relativ unwichtigen Raum kann zu einer Kompromittierung aller Telefongespräche führen
 - ★ Telefone können Überwachungsbilder anzeigen, weitere Türen öffnen etc.



Beispiel: Serverraum

- ★ Um bis in den Serverraum vorzudringen sind häufig verschiedene Sicherheitsbereiche zu überwinden
- ★ Das Entdeckungsrisiko in Serverräumen ist oft geringer als in Büros
- ★ Bei einer Entdeckung ist der Angriff dafür aber meistens komplett aufgefliegen, da eine Tarnung hier nicht möglich ist



Beispiel: Serverraum

- ★ Um bis in den Serverraum vorzudringen sind häufig verschiedene Sicherheitsbereiche zu überwinden
- ★ Das Entdeckungsrisiko in Serverräumen ist oft geringer als in Büros
- ★ Bei einer Entdeckung ist der Angriff dafür aber meistens komplett aufgefliegen, da eine Tarnung hier nicht möglich ist
- ★ Durch einen unauffällig installierten Hardwarekeylogger z.B. an lokalen Terminals werden schnell Passwörter erlangt

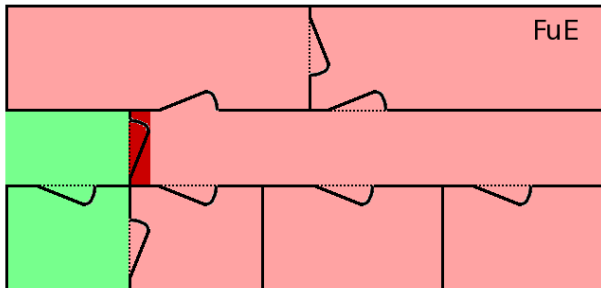




Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemeine Erfahrungen
Beispiele
Aufgefallen
Positive Erlebnisse

Beispiel: Bauliche Besonderheiten





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemeine Erfahrungen
Beispiele
Aufgefallen
Positive Erlebnisse

Beispiel: Einbruchmeldeanlagen

- ★ Einbruchmeldeanlagen sind nur sinnvoll, falls auch eine Alarmverfolgung stattfindet



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemeine Erfahrungen
Beispiele
Aufgefallen
Positive Erlebnisse

Beispiel: Einbruchmeldeanlagen

- ★ Einbruchmeldeanlagen sind nur sinnvoll, falls auch eine Alarmverfolgung stattfindet
- ★ Problem: Fehlalarme kosten Geld und werden irgendwann nur noch halbherzig oder gar nicht mehr verfolgt



Beispiel: Einbruchmeldeanlagen

- ★ Einbruchmeldeanlagen sind nur sinnvoll, falls auch eine Alarmverfolgung stattfindet
- ★ Problem: Fehlalarme kosten Geld und werden irgendwann nur noch halbherzig oder gar nicht mehr verfolgt
- ★ Also: Solange auslösen, bis Sicherheitsdienst nicht mehr erscheint



Aufgefallen, 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



Aufgefallen, 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 durch. Ich notiere Ihren Namen, damit ich sie lobend erwähnen kann. Bitte behalten sie über die Prüfung Stillschweigen, damit wir weiter testen können.“



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemeine Erfahrungen
Beispiele
Aufgefallen
Positive Erlebnisse

Positives

- ★ Gut geschulte Mitarbeiter, die Fremde direkt ansprechen
- ★ Auslösung des Alarms und Eintreffen der Security in weniger als 10 Sekunden
- ★ Mitarbeiter, die bei Geräuschen an der Türe von innen (durch die geschlossene Türe) fragen, ob sie weiterhelfen können



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemein
Türen/Fenster
Einbruchmeldeanlagen

Wie kann man sich schützen?

- ★ Vertrauen sie nicht darauf, dass ein Angreifer nicht ins Gebäude bzw. in bestimmte Räume kommt
- ★ Rechnen Sie immer damit, dass ein Angreifer Zugriff auf Ihr Netzwerk und einzelne Komponenten erlangen kann



Wie kann man sich schützen?

- ★ Vertrauen sie nicht darauf, dass ein Angreifer nicht ins Gebäude bzw. in bestimmte Räume kommt
- ★ Rechnen Sie immer damit, dass ein Angreifer Zugriff auf Ihr Netzwerk und einzelne Komponenten erlangen kann
- ★ Informieren Sie Ihre Benutzer, und stellen Sie genaue Regeln für unbekannte Personen auf
- ★ Insbesondere für Bereichen mit nur wenigen Besuchern ist dies relativ einfach



Wie kann man sich schützen?

- ★ Vertrauen sie nicht darauf, dass ein Angreifer nicht ins Gebäude bzw. in bestimmte Räume kommt
- ★ Rechnen Sie immer damit, dass ein Angreifer Zugriff auf Ihr Netzwerk und einzelne Komponenten erlangen kann
- ★ Informieren Sie Ihre Benutzer, und stellen Sie genaue Regeln für unbekannte Personen auf
- ★ Insbesondere für Bereichen mit nur wenigen Besuchern ist dies relativ einfach
- ★ Treffen Sie Vorkehrungen für den Fall, dass Hardware gestohlen wird (äquivalent zu mobiler Hardware)



(Flucht-)Türen und Fenster

- ★ Tagsüber können meistens nur einzelne Türen alarmüberwacht werden
- ★ Oft reicht hier eine akustische Alarmierung in Verbindung mit geschulten Mitarbeitern



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemein
Türen/Fenster
Einbruchmeldeanlagen

(Flucht-)Türen und Fenster





Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemein
Türen/Fenster
Einbruchmeldeanlagen

(Flucht-)Türen und Fenster





(Flucht-)Türen und Fenster

- ★ Tagsüber können meistens nur einzelne Türen alarmüberwacht werden
- ★ Oft reicht hier eine akustische Alarmierung in Verbindung mit geschulten Mitarbeitern
- ★ (Flucht-)Türen dürfen teilweise nachts abgeschlossen werden
⇒ Sprechen Sie mit Ihrer Feuerwehr



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemein
Türen/Fenster
Einbruchmeldeanlagen

Einbruchmeldeanlagen

- ★ Stellen Sie fest, wenn Unbefugte Ihre Räume betreten haben
- ★ ⇒ Einbruchmeldeanlage und Alarmverfolgung



Einbruchmeldeanlagen

- ★ Stellen Sie fest, wenn Unbefugte Ihre Räume betreten haben
- ★ ⇒ Einbruchmeldeanlage und Alarmverfolgung
- ★ Testen Sie die Effektivität Ihrer Alarmverfolgung. Wird das Gebäude überhaupt genauer untersucht, wenn keine Türen beschädigt sind?



Einführung
Einfache Werkzeuge
Angriffsziele, Theorie und Praxis
Praktische Erfahrungen
Schutzmöglichkeiten

Allgemein
Türen/Fenster
Einbruchmeldeanlagen

Fragen?

Vielen Dank für Ihre Aufmerksamkeit