

Vom mehrmals Preisgekrönten  
Wiener Neustädter Unternehmen

Damit Ihre Daten bleiben  
wohin sie gehören,

hinter Ihre FIREWALL!



## Anti-Spionage-Checks durch Hacker für jede Unternehmensgröße!

### ↳ ESCOP

Ihr Ansprechpartner im Bereich der Betriebs- und EDV- Sicherheit. Wir bieten umfassende Betriebsspionage- und Hacking-Schutzszenarien.

### ↳ Bedrohungsanalysen

Um einen Überblick über die IST-Situation zu bekommen, entwickeln wir in Bedrohungsanalysen, verschiedenen Umfangs, das derzeitige vorhandene Sicherheitsprofil.

### Wir unterscheiden hierfür vier Bereiche:

- Allgemeine Sicherheit
- Personelle Sicherheit
- Gebäudesicherheit
- Netzwerkstruktur

### Zu unserem Portfolio gehören 3 Typen von Bedrohungsanalysen:

- ♦ **SMALL** (250 Fragen)
- ♦ **MEDIUM** (450 Fragen)
- ♦ **LARGE** (NATO Standard)

### ↳ Individuelle Bedrohungsszenarien

Es gibt vielerlei Gefahrenpotential, ob aus dem Aus- oder Inland, durch Unachtsamkeit von Mitarbeitern oder bis hin zu organisierten Hacking- und Spionageversuchen. Zudem sorgen ständige Gesetzesänderungen im Datenschutz für Verschärfungen im Umgang mit Datensicherheit. Dies lässt IT-Administratoren und Geschäftsführung gleichermaßen erkennen, dass umfassende Maßnahmen bis weit außerhalb der IT-Infrastruktur notwendig sind, um Unternehmen zu schützen.

### ↳ Schwachstellen schließen

Nachdem die Bedrohungsanalyse ein umfassendes Bild der Gesamtsituation des Unternehmens in puncto Sicherheit darstellt, gilt es die vorhandenen Fehlerquellen auszubessern und zu schließen. Erst danach ergreifen wir tiefere Maßnahmen.

Aufbauend auf unsere Bedrohungsanalyse gibt es mehrere Ansätze, Ihr Netzwerk zu überprüfen.

### Je nach individuellem Bedrohungsszenario:

- ♦ **Eindringen**  
White-Box-Hacking  
Black-Box-Hacking
- ♦ **Datendiebstahl**  
Anti-Spionage-Check

### ↳ White-Box-Hacking

Ist die Simulation eines zielgerichteten Angriffs. Nachdem eine Bedrohungsanalyse durchgeführt wurde, wird hierbei jede Maßnahme die getätigt, wird im Vorhinein abgestimmt. Damit ist zu jeder Zeit transparent, was geprüft wird. Die Analyse stützt sich auf einzeln anwendbare Module, um Kosten gering zu halten.

- ♦ **Physikalische Sicherheit**  
Zutrittskontrolle  
Abhörsicherheit
- ♦ **Informelle Sicherheit**  
Datensicherheit  
Netzwerkstruktur
- ♦ **Personelle Sicherheit**  
Lieferanten, Kunden  
Mitarbeiter

### ↳ Black-Box-Hacking

Ist das Gegenteil des oben beschriebenen Szenarios. Die Aufgabe ist es, ohne weitere Informationen ein definiertes Ziel zu erreichen. Zur Zielerlangung werden alle uns zur Verfügung stehenden Mittel zur Anwendung kommen.

### Jedoch handeln wir erfolgsorientiert!

Das heißt, Sie bezahlen 50% unseres Angebotspreises. Sollte das System der Prüfung stand halten, bleibt es dabei. Falls wir das Ziel erreichen, erlangen wir somit die notwendigen Fakten, um das System ausreichend vor Angriffen zu schützen.

### ↳ Anti-Betriebsspionage-Check

Eine wachsende Gefahr sind Aktionen, die sehr gezielt und mit Hintergrundwissen erfolgen. Wir simulieren solche realen Bedrohungsszenarien aus Sicht von mehreren Perspektiven:

- Rache gekündigter oder verärgelter Mitarbeiter
- Angriff durch externe Profis (Hacker, ...)
- Angriff durch Mitbewerber

### ↳ Sicherheit herstellen

In jedem Fall erörtern wir Ihre Schwachstellen (mittels Bedrohungsanalyse) und in nachfolgenden Checks (White- & Black-Box-Hacks bzw. Anti-Betriebsspionage-Check) werden die ergriffenen Maßnahmen im Gesamtumfeld, stichhaltig auf Wirksamkeit geprüft. In weiterer Folge, erarbeiten wir mit Hilfe unserer Partner, die Lösungen, die erforderlich sind, um zu schützen, was Ihnen wichtig ist.



## Der Penetrationstest für Applikationen

### ↳ Pentest für Applikationen

Bei einem Penetrationstest für Applikationen (penetrationtest for application security) handelt es sich um einen Security-Check Ihrer eingesetzten Software.

#### Unter anderem:

- ◆ Datenbanken
- ◆ CM-Systeme
- ◆ Onlineshops
- ◆ Weblogs
- ◆ Intranet Seiten
- ◆ Kassensysteme
- ◆ Buchhaltungssoftware
- ◆ etc.

Hierbei werden Benutzerzugriffe, Verschlüsselungen, SQL-Programmierungen und vieles mehr kontrolliert. Auch können wir Belastungstests Ihrer Software durchführen, um einen Mehr-User-Zustand zu simulieren und dadurch die Sicherheit der selbigen, bei erhöhter Benutzung, feststellen zu können.

Diese Dienstleistung stellen wir ebenfalls gerne Softwareentwicklern zur Verfügung, da Sie somit Ihren Kunden ein sehr hohes Maß an Grundsicherheit gewährleisten können.

**GRATIS bei ESCOP für alle Neukunden**

Das 4 GB iPod shuffle in poliertem Edelstahl



## Sicherheitsscan Ihrer Web-Applikationen

### ↳ Eine weitere Gefahr bedroht vermehrt Unternehmen

Hacker versuchen immer öfter, über Web-Anwendungen auf sensible Daten in Systemen zuzugreifen.

Türöffner sind dabei unter anderem Programmierfehler. Anwender können reagieren, indem sie ihre Anwendungen auf Sicherheitslecks überprüfen oder Gateways dazwischenschalten.

Das ist der Alptraum jedes Unternehmens: Über eine harmlose Web-Anwendung auf seiner Homepage, die dem Kunden besseren Service bieten soll, lassen sich völlig andere, überhaupt nicht zur Veröffentlichung gedachte Informationen, aus der damit verbundenen Datenbank, auslesen.

### ↳ ESCOP bietet Sicherheits-Scans von Web-Applikationen

Mit unterschiedlichen Techniken von außen, also ohne Kenntnis des Quellcodes der Applikation, prüft ESCOP typische Schwachstellen auf Web-Anwendungs-Ebene wie z. B. SQL-Injection oder Cross-Site-Scripting (XSS).

Ausgehend vom Entry-Point arbeiten wir uns durch die erreichbaren Links und erfassen so den kompletten Aufbau der jeweiligen Web-Applikation. Um die Sicherheitslücken zu finden, penetrieren wir anschließend die Applikation mit verschiedenen Methoden.

Die so entdeckten Fehler werden genau beschrieben und je nach Zielgruppe rollen-basiert aufbereitet, beispielsweise als Compliance-Reports oder zur Fehlerbehebung für die Entwicklungsabteilung.

Wir liefern nicht nur bestmögliche Informationen über Schwachstellen, sondern unterstützen mit umfassenden Reports die folgenden Richtlinien:

- ◆ Basel II
- ◆ ISO 27001
- ◆ OWASP Top 10 2007
- ◆ The Payment Card Industry Data Security Standard (PCI)
- ◆ Klassifizierung der Websicherheitsbedrohung nach WASC

**Als Endkunde** erkennen Sie Schwachstellen stets zum frühestmöglichen Zeitpunkt und beugen damit wirksam einem Angriff vor.

**Web-Entwickler** weisen die Erfüllung von Compliance-Anforderungen nach, wenn Ihre Web-Applikation bestimmten rechtlichen oder vertraglichen Vorschriften genügen muss.

**Als Systemhaus oder ISP** bieten Sie Ihren Kunden einen besonderen Service, falls Sie Web-Applikationen Dritter hosten oder betreuen, können Sie Ihren Kunden mit unserer Hilfe den Service bieten, ihre Web-Applikationen auf Sicherheit zu überprüfen.



Treten Sie vollkommen unverbindlich mit uns in Kontakt und überzeugen Sie sich von der ESCOP eigenen Professionalität und Freundlichkeit in allen Belangen.



...denn wir sind die Guten!

### IHR ANSPRECHPARTNER

Herr Michael Kube

Mobil: +43 (0) 676 90 88 115

Fax.: +43 (0) 1 25 33 033 - 3264

E-Mail: m.kube@escop.at