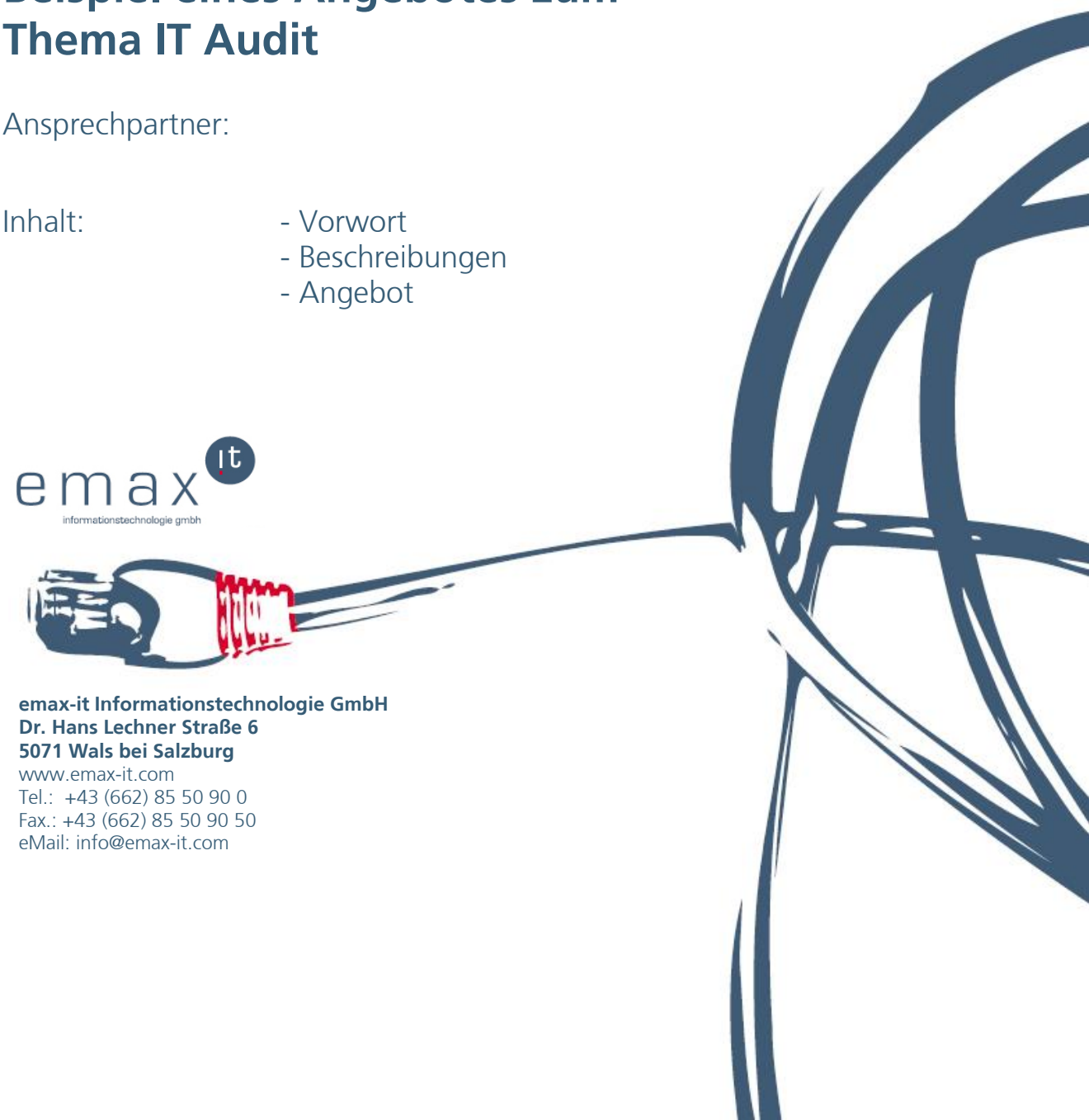
Beispiel eines Angebotes zum Thema IT Audit

Ansprechpartner:

Inhalt:

- Vorwort
- Beschreibungen
- Angebot



emax-it Informationstechnologie GmbH
Dr. Hans Lechner Straße 6
5071 Wals bei Salzburg
www.emax-it.com
Tel.: +43 (662) 85 50 90 0
Fax.: +43 (662) 85 50 90 50
eMail: info@emax-it.com

emax it
informationstechnologie gmbh

Vorwort

Seit vielen Jahren garantieren permanente Forschung und Entwicklung im Bereich IT-Sicherheit einen reichen Erfahrungsschatz der Firma emax-it Informationstechnologie GmbH.

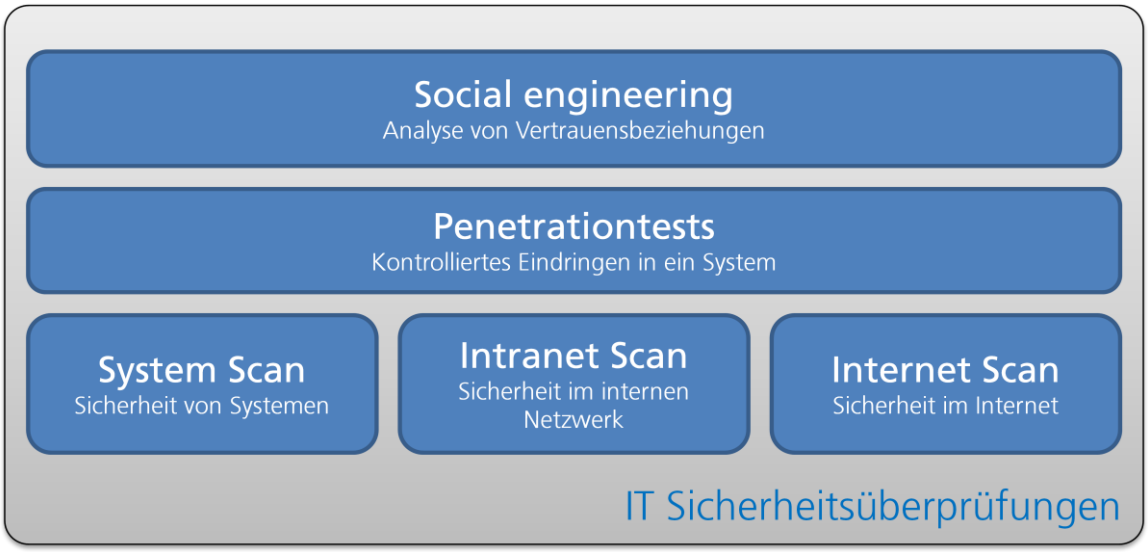
Aufgrund unserer internationalen Geschäftstätigkeit und hervorragender Spezialisten schaffen wir es stets, die besten Lösungen für unsere Kunden zu realisieren.

Wir bauen unsere Arbeitsweise auf Grundlage von persönlicher Betreuung, Qualität und Transparenz und machen somit unsere Leistungen von Beginn an messbar.

Ein angemessenes IT-Sicherheitsniveau kann daher in zunehmendem Maße nur durch übergreifendes Fachwissen und organisiertes Vorgehen erreicht und aufrechterhalten werden.

Das Ergebnis unserer Prüfungen wird immer in einem Management Report / Detailreport zusammengefasst und mit den gesammelten Rohdaten dem Kunden übergeben.

Überblick über unsere Dienstleistungen im Bereich IT Sicherheit



1. System Scan

Kritische Computersysteme (Netzwerkserver, Webserver u.a.) sollten nach dem Minimumprinzip konfiguriert werden. Oftmals reicht eine out-of-the-box-Installation nicht aus, um einen Server "sicher" zu konfigurieren:

- Es sind Sicherheitspatches zu installieren,
- Dienste zu deaktivieren,
- Systemparameter zu setzen oder
- Berechtigungen zu setzen.

Bei dieser Prüfung werden diese Systeme einer genauen Konfigurationsprüfung unterzogen. Ziel dieses Arbeitspaketes ist, eine möglichst ausführliche Analyse der Schwachstellen zu erhalten.

Die Optik ist auf die korrekte und sichere Konfiguration eines bestimmten Betriebssystemtyps (UNIX, Linux, Windows Server) und/oder Anwendungen (Exchange, Oracle, DB2) gerichtet und es wird gefragt: "Wo sind meine Schwachstellen?".

Die Schwachstellen werden nach Herkunft kategorisiert und für jede Kategorie (oder wo sinnvoll für jede einzelne Schwachstelle) wird eine klassifizierte Empfehlung zur Behebung der Gefährdung angegeben. Die Klassifikation der Empfehlung orientiert sich an den beiden Dimensionen Wichtigkeit und Dringlichkeit.

2. Intranet Scan

Ein Intranet-Scan ist im Wesentlichen dasselbe wie der Internet-Scan (Arbeitspaket 3), diesmal aber innerhalb des Netzwerkes. Er umfasst die automatisierte Suche nach Computersystemen und Netzwerken die intern sichtbar und zugänglich sind. Es werden alle von innen sichtbaren Komponenten identifiziert und auf derzeit bekannte Schwachstellen untersucht.

Ziel dieses Arbeitspaketes ist eine möglichst ausführliche Analyse der von innen zugänglichen Systeme. Die Auffälligkeiten werden nach Herkunft kategorisiert und für jede Kategorie wird eine klassifizierte Empfehlung zur Behebung der Gefährdung angegeben.

3. Internet Scan

Ein Internet-Scan umfasst die Suche nach Computersystemen und Netzwerk-Infrastrukturkomponenten über das Internet. Es werden alle von extern sichtbaren Komponenten identifiziert und auf derzeit bekannte Schwachstellen untersucht.

Schwachstellen können verschiedenster Herkunft sein (z.B. Design, Implementation oder Konfiguration); sie haben je nachdem geringere oder größere Auswirkungen auf die Gefährdung der betroffenen Komponente und des betroffenen Netzwerkes.

Entsprechend werden Schwachstellen auch als "high", "medium" oder "low severity" klassifiziert. Ziel dieses Arbeitspaketes ist, eine ausführliche Analyse der von außen zugänglichen Systemen zu erhalten.

4. Penetrationtests

Der Penetrationtest umfasst den Versuch, eine identifizierte Schwachstelle auszunützen und so weit wie möglich in das System einzudringen. Ziel dieses Arbeitspaketes ist also, aufzuzeigen, wie weit in das interne Firmennetzwerk eingedrungen und welcher Schaden angerichtet werden könnte. Als Grundlage können dazu die Ergebnisse der Arbeitspakete 1 bis 3 dienen.

Abgrenzung: Es werden nur solche Methoden verwendet, die keinen Schaden an Systemen oder Daten verursachen. Es werden explizit keinerlei Daten gelöscht oder verändert, sondern höchstens darauf hingewiesen, dass dies auf diese oder jene Art und Weise möglich ist!

4.1. Details zu Penetrationtests (automatisiert und manuell)

- Server Patch Level
  - Ausnützen bekannter Sicherheitslücken
- Network- Transport- Session-Layer Protokoll
  - UDP Packet Storms
  - TCP SYN Flooding
  - ICMP-Echo Reply Packet
- Konfiguration
  - Enumeration von Server-Inhalten
  - Ausnutzen Default Accounts
  - Enumeration von Benutzeraccounts
  - Ausnutzen von Protokollfeatures

  - Ausnutzen falsch gesetzter Berechtigung
  - Ungeschützte Funktionalität
  - Enumeration von Server-internen Informationen
  - Passwörter erraten

- Umgehen der Authentisierung
- Zugriff auf geschützte Funktionalität/Ressourcen
- Sammeln von Infos über Entwickler Kommentare
- Sammeln von Infos über System- oder Fehlermeldungen
- Lesen alter unreferenzierter Files
- Diverses (etwa Upload beliebiger Files...)
- Aufbrauchen limitierter Ressourcen
- Aussperren von Benutzeraccounts
- Zugriff Dateisystem
- Code Injection
- Command injection
- Format String Injection
- IMAP/SMTP Injection
- Overflowing Char Buffers
- Path Traversal
- SQL Injection
- SSI Injection
- Client-seitige Attacken
  - Cross Site Request Forgery (XSRF)
  - HTML Injection /Cross Site Scripting (XSS)
  - HTTP Response Splitting / header injection
  - Session fixation

5. Social engineering

Von Social Engineering spricht man immer dann, wenn ein Angreifer, menschliche Eigenschaften ausnutzt um an Informationen zu gelangen. Social Engineering Angriffe sind eine effiziente Methode zur Informationsbeschaffung und zwar ohne Einsatz von technischen Hilfsmitteln.

Angreifer nutzen dafür natürliche menschliche Reaktionen aus, positive Eigenschaften wie Hilfsbereitschaft, Kundenfreundlichkeit, Dankbarkeit, Stolz auf die Arbeit und das Unternehmen.

Ziel dieses Arbeitspaketes ist, einen klaren Überblick über die „Sicherheitskultur im Unternehmen" zu erhalten um gezielt das Unternehmen gegen ungewollten Informationsaustritt zu schützen.

6. Inhaltliches Angebot

Folgende Punkte werden in diesem Angebot detailliert.

6.1. Externer Scan: Penetrationtest I der Systeme, welche per Internet erreichbar sind

Nähere Details in Punkt 4.
Durch den Penetrationstest versucht emax-it den kontrolliert, von „außen" in ein bestimmtes Computersystem oder Netzwerk einzudringen, um Schwachstellen zu identifizieren. Dazu werden gleiche bzw. ähnliche Techniken eingesetzt, die auch bei einem realen Angriff verwendet werden. Die hierbei identifizierten Schwachstellen können dann durch entsprechende Maßnahmen behoben werden, bevor sie von unautorisierten Dritten missbraucht werden können.

Die Tests werden auf den unten angeführten Ebenen durchgeführt.

- **Betriebssystem**
  Version und bekannte Schwachstellen (sog. Exploits)
- **Dienste**
  Arten, Versionen und bekannte Schwachstellen
- **Firewall**
  Art der Firewall, Regelwerk und Umgehung (sog. Evasion)
- **Anfälligkeit für verschiedene Angriffe aus der Anwendungsschicht**
  Cross-Site-Scripting (XSS), SQL-Injection, Path Disclosure, Remote File Inclusion, Directory Traversal, ...

Zu prüfende Systeme:

Der Prüfungsumfang umfasst folgende Netze:

…

6.2. (Optional) Externer Scan: Penetrationtest II (wie 6.1)

Optional wird der Test der bekanntgegebenen Raiffeisen Server angeboten.

Zu prüfendes System:

Der Prüfungsumfang umfasst folgende Netze:

6.3. Social Engineering

Folgende Bereiche werden hierbei getestet:

- Informationsbeschaffung im Internet über Mitarbeiter und Vorstände
  - Google, Yahoo, Xing, Facebook
- Informationsbeschaffung Vor-Ort
  - Shoulder Surfing,
  - Test der Zugangskontrollen,
  - Vortäuschen einer falschen Identität (intern, extern),
  - Versuch an Rechner im internen Netzwerk Zugriff zu erlangen.
- Angriffswelle über Internet
  - Informationsbeschaffung über Email
- Angriffswelle über Telefon
  - Vortäuschen falscher Identitäten
  - Allgemeines Interesse an Dienstleistungen
  - Erhalt von sensiblen Geschäftsinformationen

Diese oben genannten Maßnahmen, werden im Vorfeld abgeklärt und besprochen um die Vorgehensweise im Detail zu klären.

7. Aufwände für die Tests

8. Details der Budgetierung