Wir von Amenaza Technologies und der m-privacy GmbH fühlen uns Ihnen gegenüber verpflichtet auf allen unseren Gebieten bestmöglichste Ergebnisse zu erzielen. Sei es die technische Unterstützung, das Update der Bibliotheken oder unser Kundenservice. Wir arbeiten mit Ihnen, um Ihnen das Beste aus unseren Produkten zu bieten.

KONTAKT:

m-privacy GmbH

Am Köllnischen Park 1
D - 10179 Berlin

Tel: +49 30 243 423 34
Fax: +49 30 243 423 36

E-MAIL: info@m-privacy.de
WEB: http://www.m-privacy.de

Amenaza Technologies Limited
550—1000 8th Avenue SW
Calgary,AB Canada T2P3M7

Tel: +1 (403) 263-7737
Fax: +1 (403) 278-8437
Toll-Free 1-888-949-9797

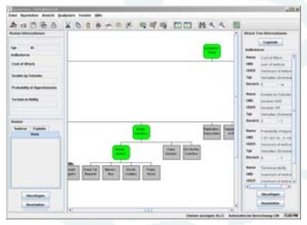
E-MAIL: info@amenaza.com
WEB: http://www.amenaza.com

Informationstechnologie

In der vernetzten Welt ist Risiko heute nicht nur eine Gefahr, sondern eine Tatsache.

Viele Unternehmen versuchen ihr Risiko „zu minimieren". Doch dieser Ansatz hat keinen Erfolg, sondern führt zu Rentabilitätsverlusten und verliert sich in unausgewogenen Maßnahmen. Ein viel effektiverer Ansatz ist das Risiko zu „optimieren".

Die Risikooptimierung geht davon aus, dass alle unternehmerischen Aktivitäten, ein gewisses wirtschaftliches Risiko mit sich bringen. Ein optimales Risikolevel ist also in der Lage Gewinne über einen langen Zeitraum zu maximieren **und** dabei gelegentliche Vorfälle mit begrenztem Einfluss als notwendiges Übel mit einzukalkulieren. Als Unternehmen profitieren Sie dann am meisten, wenn Sie ihr Sicherheits-Budget in Technologien investieren, die unnötige und außergewöhnlich hohe Risiken ausschließen.



Amenaza Technologies hat mit ***SecurITree*** das erste kommerzielle Attack Tree basierte Risikoanalyseprogramm und die dazugehörige Methodologie entworfen. Es erlaubt Ihnen die Risiken von IT-Systemen zu analysieren und zu verstehen. ***SecurITree*** analysiert den Aufbau eines Systems und ist damit ein strategisches Planungsinstrument für die Analyse des bestehenden Systems und für die Effektivität neuer Sicherheitslösungen.

DURCH DEN EINSATZ EINER ANSPRUCHSVOLLEN MODELL-TECHNIK, der „Attack Tree Analyse", kann *SecurITree* dem IT-Spezialisten Risiken grafisch aufbereiten.

Die Methodologie im einzelnen:

- Die grafische Darstellung von Schwachstellen im IT System anhand des Attack Tree Modells
- Erkennen von Personen und Ereignissen (Bedrohungsagenten), die das IT-System bedrohen
- Erstellen einer mathematischen Formel um die Möglichkeiten der Bedrohungsagenten den Schwachstellen des IT Systems gegenüber zu stellen
- Aufdecken der Schwachstellen, die am wahrscheinlichsten einem Angriff ausgesetzt sind
- Ausschließen von unwahrscheinlichen Bedrohungen
- Entscheiden welche der verbleibenden Bedrohungen gefährlich werden könnten
- Unterstützen des Entscheidungsprozesses und die Schaffung einer IT-Security-Policy, die gleichermaßen den technischen Experten als auch dem Management unmittelbar zugänglich ist

Das systematische und grafische Attack Tree Modell von SecurITree erlaubt Ihnen zu bestimmen, welche Bedrohungen am wahrscheinlichsten auftreten werden. Indem Sie Knoten „schneiden", die von Ihren Feinden unmöglich erreicht werden können, erkennen Sie welche Bedrohungen irrelevant sind. Die verbleibenden Knoten werden dann ausgewertet, um zu bestimmen, ob das Risiko tragbar ist oder unbedingt ausgeschlossen werden muss.
SecurITree hilft das optimale Risikolevel zu bestimmen. Unternehmen profitieren davon, indem sie ihre eigene IT-Sicherheitsressourcen entwickeln, um unnötige und außergewöhnlich hohe Risiken auszuschließen.

Attack Trees selber erstellen

SecurITree ermöglicht es Ihnen einfach und schnell Attack Tree Modelle für Ihre IT-Systeme zu erstellen. Die Attack Trees passen sich **Ihrem** Systemplan und neuen Implementierungen an, nicht irgendwelchen Allgemeinen. Die Analyse basiert auf dem Wissen über Ihre Feinde. Mit *SecurITree* sind Sie in der Lage Ihre Bedrohungs- und Gefährdungslage einzuschätzen.

Attack Tree Bibliotheken

Selbst Individualsysteme, die nach Wünschen des Kunden erstellt worden sind, greifen auf viele Standardkomponente zurück (z.B. Oracle, Solaris, Windows 2000). Das Modellieren jedes dieser Systeme von Grund auf neu wäre eine Syssyphos Arbeit und benötigte spezielle Fachkenntnisse. *SecurITree* bietet eine Anzahl von Attack Tree Bibliotheken[1], auf die Sie zurückgreifen können. Die Attack Trees aus den Bibliotheken können leicht eingebunden und einfach angepasst werden. Die Bibliotheken werden regelmäßig erneuert und erweitert, um mit neuen Bedrohungssituationen Schritt halten zu können. *SecurITree* Kunden haben exklusiven Zugriff auf diese Bibliotheken, die ein Baustein der *SecurITree-Software* ist.

Recycling von Wissen

SecurITree ermöglicht es Ihnen Bibliotheken zu erstellen und darin eigene Konfigurationen zu sichern. Darauf können dann andere Personen oder Abteilungen in Ihrem Unternehmen aufbauen und diese an neue Problemstellungen anpassen.

1 Bei Interesse an genaueren Details kontaktieren Sie bitte die m-privacy GmbH

Stabile Grundlagen helfen beim Entscheidungsprozess

Versichern Sie sich, dass Ihre Entscheidungen bei der Risikoanalyse in einem systematischen und logischen Prozess begründet sind, die alle Interessensvertreter berücksichtigen. *SecurITree* macht es möglich:

WISSEN: Umfassende Modellierung der Risiken Ihres IT-Systems.

EINBINDUNG: Berücksichtigung verschiedener Risikobewertungen der IT-Abteilung und der Unternehmensleitung.

ENTSCHEIDUNGSGRUNDLAGE:
Benutzen Sie vollständige Attack Trees zur Findung und Unterstützung des Entscheidungsprozesses.
Wer wird angreifen? Welche Schwachstellen können ausgenutzt werden? Sollte das Risiko entschärft werden? Wie können die Löcher im Systems geschlossen werden?

DELIGIERUNG: Attack Trees sind natürliche Delegationswerkzeuge. Ordnen Sie Äste des Modells relevanten Abteilungen oder Funktionsträgern zu.

INFORMATIONSSTAND: Attack Trees wachsen mit neuen Risiken; Gefahren werden ausgeschaltet wenn Risiken benannt werden... Sie werden aber immer den Überblick behalten und können dies auch transparent machen.

WAGEN SIE ES
DAS RISIKO EINZUGEHEN ?

Erfahren Sie die Antwort
mit SecurITree