INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Newsletter 1.03

In diesem Newsletter finden Sie Antworten zu den folgenden Fragen:

:: IT-Sicherheit: Was bedeutet dies für mein Unternehmen?

:: Was sind Patches?

:: Wieso werden immer neue Software-Lücken bekannt?

:: Woher bekomme ich Sicherheits-Informationen?

:: Was muss ich im Zusammenhang mit Patches beachten?

Dies ist eine kostenlose Dienstleistung von der GO OUT Production GmbH.

Inhaltsverzeichnis

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 IT-Sicherheit: Was bedeutet dies für mein Unternehmen?

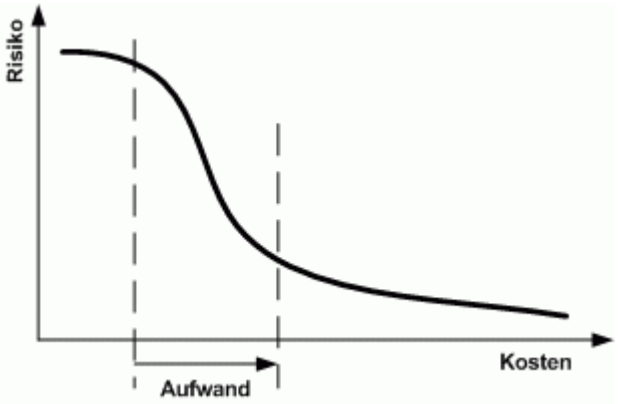
Die Wahrnehmung von Sicherheit ist subjektiv.
Was für die eine Person als sicher gilt, muss für die andere noch lange nicht entsprechend wirken.

Ein Mitarbeiter der amerikanischen National Security Association NSA hat "sicher" einmal wie folgt umschrieben: Ein Computersystem, das sich in einem bombensicheren Bunker 100 Meter unter der Erdoberfläche befindet und keine Anschlüsse zur Aussenwelt aufweist, ist sicher. Wobei er nicht unterliess anzufügen, er wisse nicht, ob dies auch wirklich sicher sei…

Der Duden definiert Sicherheit als Sammelbezeichnung für Verfahren und Einrichtungen, mit denen zum Beispiel Datensicherheit und Dateischutz gewährleistetwird.

Direkt abhängig vom eigenen Sicherheitsbedürfnis sind Kosten und Nutzen der erforderlichen Massnahmen. Immer neuere Systeme und Methoden helfen, bestehende Infrastrukturen sicherer zu machen. Doch nicht immer lohnt sich der Aufwand.

Wichtig ist, dass man das Risiko, welches man einzugehen gewillt ist, kennt und akzeptiert.



Sicherheit ist ein steter Prozess und nicht ein Produkt. Täglich werden neue Soft- und Hardwarelücken bekannt, Angriffe auf Netzwerke nehmen laufend andere Formen an.

Nur wer am Ball bleibt, kann sich optimal darauf einstellen und sich auch dagegen schützen.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

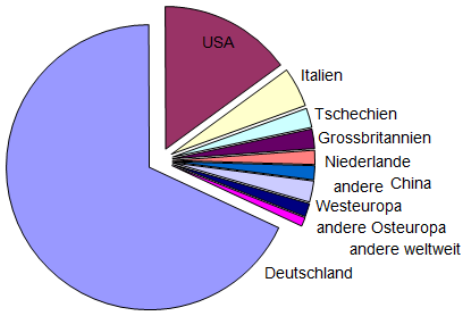
Telefon 052 320 91 20
Fax 052 320 91 21

2 Wieso werden immer neue Software-Lücken bekannt?

Softwarehersteller stehen unter einem enormen Konkurrenzdruck. Ihr Produkt muss vor allen anderen auf den Markt sein, um nicht wichtige Kunden zu verlieren.

Wo kommen die Hacker her?

Deutschland	68 Prozent
USA	15 Prozent
Italien	4.5 Prozent
Tschechien	2.2 Prozent
Grossbritannien	2.2 Prozent
Niederlande	1.6 Prozent
China	1.6 Prozent
andere Westeuropa	2.4 Prozent
andere Osteuropa	1.5 Prozent
andere weltweit	1 Prozent



Dieser Zeitdruck wirkt sich auf die Programmierer aus. Es ist nicht mehr möglich, alle Funktionen bis ins kleinste Detail zu testen. Und auch der Programmcode wird immer umfangreicher und komplizierter. Da den Überblick zu behalten, ist nicht einfach, gerade wenn noch eine gewisse Unwissenheit dazu kommt. Das bietet Hackern die Gelegenheit, mögliche "undefinierte" Funktionen auszunützen und zu manipulieren.

3 Was sind Patches?

Sobald Software-Löcher bekannt sind, versuchen die Hersteller, diese zu "stopfen". Die dafür entwickelten Programmteile nennt man Patches, sogenannte "Software-Flickwerke".

Es ist enorm wichtig, Patches auch aufzuspielen. Ein Paradebeispiel war unlängst der Wurm SQL-Slammer. Er nutzte ein seit Mitte 2002 bekanntes Sicherheitsloch des SQL-Servers von Microsoft. Da nur wenige Unternehmen den zur Verfügung gestellten Patch auch verwendeten, verbreitete sich der Wurm rasend schnell. In der ersten Nacht konnte er über 160'000 Systeme befallen. Insgesamt hat er laut Analysten und Sicherheitsexperten über 1.2 Milliarden US-Dollar Schaden verursacht.

Solche Löcher helfen auch Skript-Kiddies, in ein System einzudringen. Skript-Kiddies benutzen im Internet frei verfügbare Software, ohne selber die Technik dahinter zu verstehen. Die Software lässt sich ohne Aufwand innert Minuten finden und sofort einsetzen. Damit greifen sie ohne ein bestimmtes Ziel beliebige Rechner an, wobei es unwichtig ist, ob es sich dabei um Rechner von Privatpersonen oder Unternehmen handelt.

Auch diese Gefährdung muss bei der Festlegung der eigenen Sicherheit-Standards berücksichtigt werden.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4 Woher bekomme ich Sicherheits-Informationen?

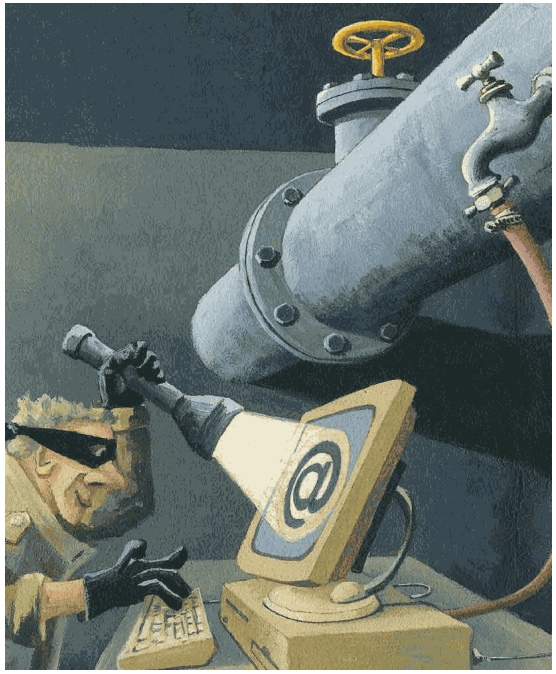
Alle Software-Hersteller sind sich dieser Risiken bewusst. Wird eine neue Lücke bekannt, versuchen Sie, möglichst schnell einen Patch zu entwickeln. Ist dieser verfügbar, informieren sie umgehend via Homepage und Newsletter ihre Kunden. Von daher ist es wichtig, sich in die Newsletter-Liste der Hersteller einzutragen,
um stets auf dem aktuellsten Stand zu bleiben.

Es ist Aufgabe der Security-Internetseiten, diese Informationen zusammenzutragen.

Auf unserer Homepage http://www.goSecurity.ch erfahren Sie, wenn ein neuer Patch vorhanden ist. Eine spezielle Rubrik bezieht sich ausschliesslich auf die Microsoft-Betriebssysteme (Rubrik: MS-Patches).

Im Internet finden Sie auch spezialisierte Newsletter für Profis. Einer der bekanntesten heisst Bugtraq. Sobald jemand ein neues Loch gefunden hat, informiert er die gesamte News-Group, um so das neueste Wissen gleich auszutauschen.

Für die Überprüfung der Sicherheitsstandards im Unternehmen selbst gibt es verschiedene Tools. Ein solches kostenloses Tool, der "Microsoft Baseline Security Analyzer" zeigt auf, wie sicher der eigene Computer konfiguriert ist und gibt Ratschläge zur Optimierung.



goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

5 Was muss ich im Zusammenhang mit Patches beachten?

Leider kann es geschehen, dass auch Patches Fehler enthalten oder neue Löcher öffnen. Es empfiehlt sich daher, neue Patches zuerst in einer Testumgebung auszuprobieren. Microsoft zum Beispiel musste dieses Jahr bereits drei Patches infolge massiver Probleme zurückziehen.

Newsletter informieren auch hier, wann ein Patch in Ordnung ist (oder eben nicht).

Warten Sie jedoch nicht zu lange mit dem Aufspielen. Innert weniger Tage finden Sie im Internet Tools, die erkennen können, ob auf dem anzugreifenden System dieses "Loch" noch offen ist oder nicht.

Nicht alle Systeme sind gleich gefährdet. Legen Sie Ihr Augenmerk vor allem auf die unersetzbaren Komponenten wie zum Beispiel Firewall, Netzwerkelemente und das Betriebssystem. Sie sind besonders gefährdet.

Achten Sie bei allen Programmen, die eine Verbindung ins Internet aufbauen, darauf, dass diese aktuell sind. Hierzu zählen unter anderem die Browser (Internet Explorer, Netscape, Mozilla, Opera…), File-Sharing-Tools oder Messaging Systeme. So können mögliche Gefährdungen bereits von allem Anfang an deutlich minimiert werden.