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.

Die Firewall – das zentrale Security-Element

Die Firewall ist das zentrale Netzwerkelement, um die Sicherheit für ein Unternehmen aus Sicht der IT sicherzustellen. Dabei wird diesem Element aber oft zu wenig Aufmerksamkeit geschenkt. Der Schutz ist nur so gut wie die Firewall bzw. deren Einrichtung.
Die Firewall muss alles „böse" filtern und nur die „guten" Pakete in das Netzwerk hereinlassen. Dazu gibt es auf dem Markt eine Vielzahl von Produkten, die die Wahl zur Qual machen. Dieses INFONEWS hilft Ihnen, sich in diesem Dschungel zu Recht zu finden und eine optimale Konfiguration vorzunehmen.

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

Inhaltsverzeichnis

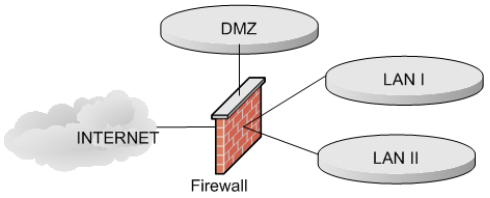
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Die richtige Firewall

Die wichtigste Frage ist die Wahl nach der richtigen Firewall: eine Softwarelösung oder eine Hardwarelösung? Während für den Heimgebrauch eine Softwarelösung Sinn macht, kann diese Lösung den Anforderungen im Business-Umfeld oft nicht genügen. Hier muss eine Hardwarelösung eingesetzt werden. Die Anforderungen an eine Firewall sind dabei zahlreich und können hier nicht bis ins letzte Detail behandelt werden. Definieren Sie im Vorfeld, wie viele Netzwerksegmente an die Firewall kommen. Je mehr Zugänge Sie haben, umso teurer wird auch die Firewall (und umso weniger Produkte stehen zur Auswahl). Für die meisten Unternehmen reichen drei Segmente: Internet, LAN und DMZ. In die DMZ kommen typischerweise Server, die von Aussen erreichbar sein müssen, wie Web- oder Emailserver, hin.



Viele Firewall-Hersteller liefern Ihre „Feuermauer“ in einer eigenen Box, mit einem eigenen Betriebssystem. Hier wurde nur installiert, was wirklich benötigt wird. Dies macht die Angriffsfläche sehr klein. Eine Firewall auf einem ungepatchten Windows 2000 wird hingegen nie die Sicherheit bieten können, die Sie benötigen und erwarten.

Hardware Firewall

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Wenn Sie eine Softwarelösung einsetzen, achten Sie darauf, dass die Grundlage, sprich das Betriebssystem, auf dem aktuellsten Stand ist und alle nicht benötigten Dienste deaktiviert oder noch besser deinstalliert sind. Nur eine „saubere" Basis garantiert, dass die Firewall korrekt und ohne böse Überraschungen arbeiten kann. Jedes noch so kleine Zusatzprogramm bietet eine unnötige Angriffsfläche.

Bei der Wahl der richtigen Firewall spielt auch die Art der Konfiguration eine wichtige Rolle. Die meisten Firewalls sind von Beginn weg geschlossen, das heisst, mit den selber definierten Regeln öffnet man Zugänge. Einige wenige Produkte arbeiten gerade umgekehrt, sie sind offen wie ein Scheunentor und mit den Regeln wird nach und nach die Türe geschlossen. Die letzte Regel muss immer alles schliessen.

2 Was macht eine Firewall?

Jede Firewall arbeitet nach dem gleichen Prinzip: Die Eintrittspunkte aus dem Internet in ein lokales Netzwerk werden auf einen Punkt minimiert. Die Firewall entscheidet nach den von Ihnen definierten Regeln, ob eine Verbindung durch die Firewall zugelassen wird oder geblockt werden muss. Sie kann aber nicht unterscheiden, ob das Paket korrekt ist oder ob dieses bösen Code beinhaltet. Aus diesem Grund werden auch Virenverseuchte Emails nicht gefiltert. Dazu sind zusätzliche Elemente notwendig, die diese Aufgabe übernehmen.
Da gibt es zum Beispiel einen einfachen SMTP Filter oder einen SMTP Proxy.

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3 Wie erstelle ich ein Firewall-konzept?

Das Öffnen (bzw. Schliessen) von Ports (oder so genannten Diensten) muss sehr genau überlegt werden. Diese Aufgabe ist von zentraler Bedeutung. Ohne diese Planung kann keine korrekte Einstellung garantiert werden und es öffnen sich Schwachstellen.

Überlegen Sie sich zuerst, welche Verbindungen von Aussen nach Innen benötigt werden. Haben Sie keinen Server in der DMZ, muss auch kein Port geöffnet werden. Öffnen Sie nur, was wirklich offen sein muss. Wenn Sie keinen eigenen Mailserver betreiben, erübrigt es sich auch, diesen Port zu öffnen.
Nachfolgend ein Muster, wie vereinfacht die Regeln für ein kleines Unternehmen mit einem Mailserver im LAN aussehen können.

LAN – Internet

Nr.	Bezeichnung	Quelle	Ziel	Port
Out.1	http	Arbeitsstation	Any	HTTP(80), SSL(443)
Out.2	Mail	Mailserver	Provider oder ev. Any	SMTP(25)
Out.3	DNS	Domaincontroller	ns1.ip-plus.net ns2.ip-plus.net ns3.ip-plus.net	DNS(53)
Out.4	NTP-Client	Arbeitsstationen	Swisstime.ethz.ch	NTP(123)
Out.5	NTP-Server	Server	Swisstime.ethz.ch	NTP(123)
Out.6	…			

Bemerkung: Es dürfen nur Arbeitsstationen ins Internet. Den Servern bleibt dies aus Sicherheitsgründen verwehrt.

Internet - LAN

Nr.	Bezeichnung	Quelle	Ziel	Port
In.1	Mail	Any	Mailserver	SMTP
In.2	….			

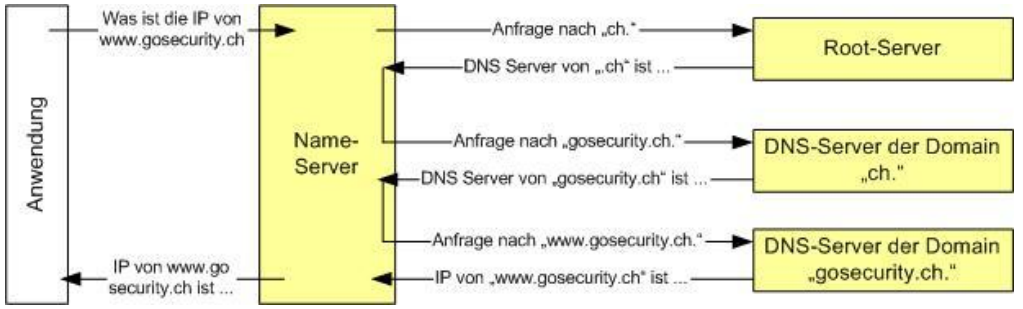
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Von Aussen ins LAN wird in der Regel keine Verbindung benötigt. Oft wird z.B. der Port 80 (http) geöffnet, weil Internetverbindungen von den Mitarbeitern ins Internet gehen müssen und die Antwort durch diese Regel garantiert wird. Eine Firewall merkt sich jedoch, wer eine Verbindung ins Internet geöffnet hat und schickt die korrekte Antwort an den anfordernden PC zurück. Die Regel, z.B. das Öffnen des Port 80 von aussen nach innen, ist daher nicht notwendig und muss unbedingt entfernt werden. Sollten Sie wirklich eine Verbindung vom Internet ins LAN benötigen, versuchen Sie diese Verbindung einzuschränken. Sie können dies z.B. auf eine IP-Adresse oder noch besser eine MAC-Adresse beschränken. IP sowie MAC Adressen können zwar gefälscht werden, ein potentieller Angreifer bekommt jedoch keine Antwort auf seine Anfrage, da das Paket nicht mehr richtig zurück geroutet werden kann.

Von der DMZ ins Internet muss im Normalfall ebenfalls kein Port geöffnet sein. Hier gibt es Ausnahmen, wenn ein Mailserver betrieben wird. Dieser muss seine Emails ja verschicken können. Bevor er dies macht, benötigt er die IP-Adresse zur entsprechenden Email-Adresse. Dies wird via DNS erledigt (Port 53). Achten Sie hier darauf, dass der Port 53 nicht global offen ist, sondern klar eingeschränkt wird. Ihr Internet-Provider hat einen DNS Server, den Sie als „Weiterleitungsserver" benutzen dürfen. Schränken Sie den Zugriff nach Aussen nur auf diese einzige Maschine ein. Viele Hackertools nützen genau diese Schwachstelle aus und verschicken vertrauliche Informationen via Port 53 an den Angreifer zurück!
Für die Verbindungen auf einen Webserver gilt wiederum der gleiche Umstand wie vom LAN ins Internet. Auch hier muss der Port 80 von der DMZ ins Internet nicht geöffnet werden, da ein Webserver vom Internet aufgerufen wird, aber der Webserver nichts aus dem Internet Aufzurufen hat.



Ablauf DNS Auflösung über einen Name Server

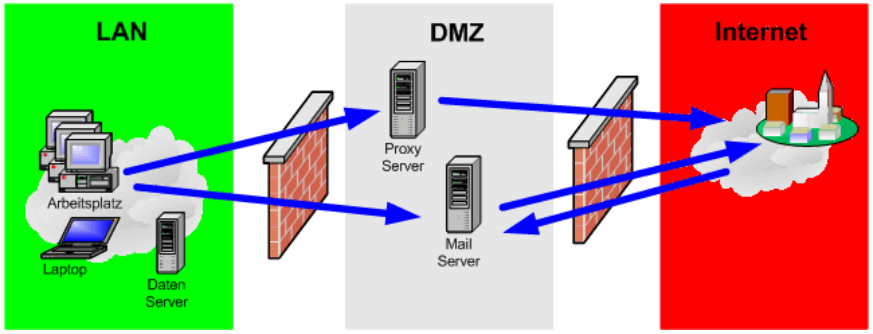
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Vom LAN ins Internet ist oft eine Vielzahl von Ports offen. Dies muss jedoch nicht sein. Mailverbindungen z.B. müssen nur in die DMZ gelangen, falls dort ein Mailserver steht. Dieser schickt dann das Mail an die korrekte Adresse weiter. Ebenfalls muss die Firewall nicht für jeden Arbeitsrechner den Port 80 (http) geöffnet haben. Setzen Sie zur Sicherheit einen Proxy ein. Nur dieser Server darf dann ins Internet und die entsprechende Seite holen. Der Proxy-Server gehört wiederum in die DMZ.

Fassen Sie bitte nicht zu viele Regeln zusammen. Die Übersichtlichkeit ist zwar viel besser vorhanden, jedoch ist es schwer, auf einen Blick zu erkennen, wer nun wirklich diese Regel benutzen kann (und darf) und wer nicht. Bilden Sie nur Gruppen, wo es zwingend notwendig ist und Sinn macht. Oft werden ganze Domainen zusammengefasst und freigegeben. Ein Mitarbeiter kann diesen Umstand ausnutzen und seinen Rechner in diese Domaine zügeln (z.B. IP Adresse ändern) und so Zugriffe erlangen, die nicht erlaubt sind.



goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4 Vorgehen

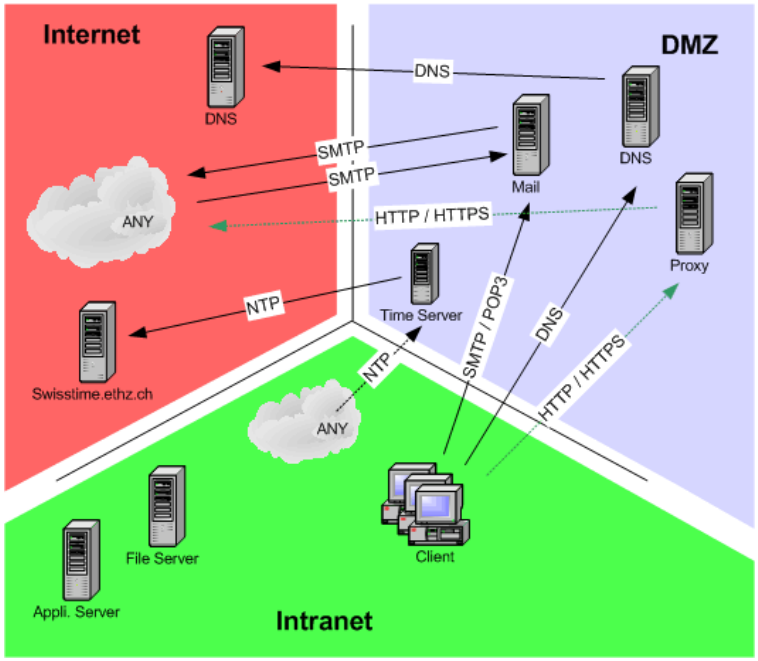
Um optimale Gruppen zu bilden, gehen Sie wie folgt vor:

1. Unterteilen Sie ein grosses Blatt Papier (A3 oder grösser) in drei Teile ein und betiteln Sie diese Teile mit Internet, LAN und DMZ (falls Sie mehr Zugänge haben, teilen Sie das Blatt in die entsprechende Anzahl Zugänge ein)

2. Zeichnen Sie nun in jeder Zone die vorhandenen Rechner und Server ein. Bezeichnen Sie diese mit der Funktion und der IP-Adresse.

3. Zeichnen Sie nun alle Verbindungen zwischen den Rechnern und Servern ein. Beachten Sie auch, dass Verbindungen zu bestimmten Rechnern im Internet möglich sind, z.B. zu einem Zeitserver (z.B. NTP Port 123). Mit einem Pfeil kennzeichnen Sie die Richtung der Verbindung (z.B. vom LAN in die DMZ, von der DMZ ins Internet usw.). Schreiben Sie zu jedem Pfeil, welchen Dienst, bzw. welchen Port diese Verbindung benutzt (z.B. 80 oder http, 25 oder smtp, usw.). Zeichnen Sie mehrere Pfeile, wenn diese Verbindung für mehrere Ports benutzt wird.

4. Versuchen Sie nun, sinnvolle Gruppen zu bilden. Dies macht z.B. bei Arbeitsplatzrechnern Sinn. Beschränken Sie aber die Gruppe auf die vorhandenen Rechner und öffnen Sie nicht einen ganzen Bereich, z.B. mit der Subnetzmaske 255.255.255.0 für alle Rechner von x.x.x.1 bis x.x.x.255.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

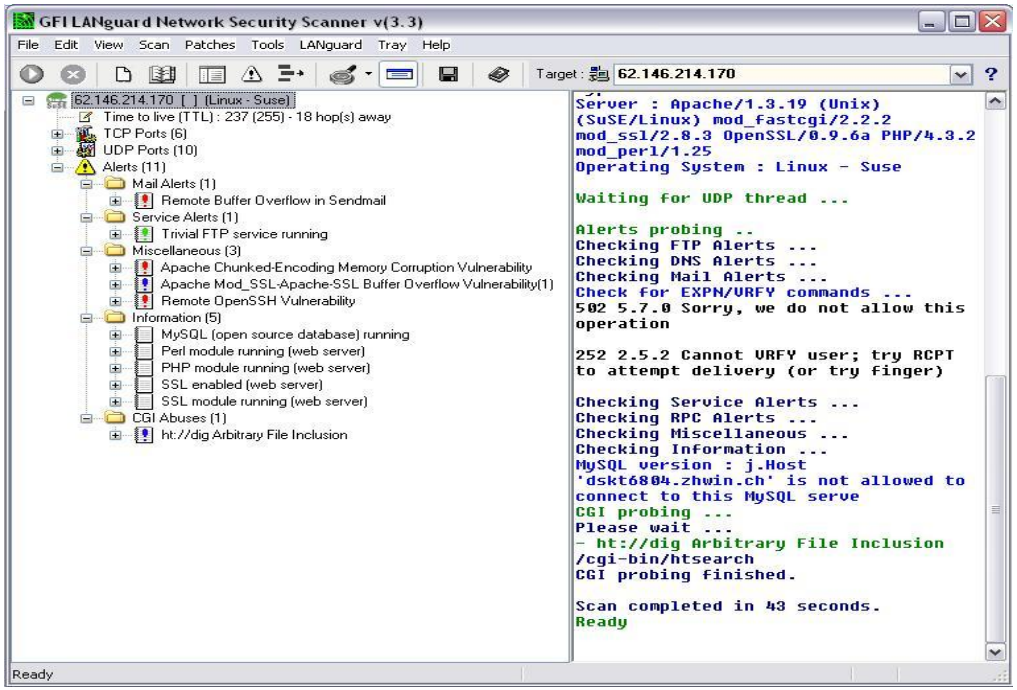
5. Kontrollieren Sie nochmals alle Verbindungen und Gruppen. In über 90% der Firewall Konzepte gibt es keinen Pfeil der aus dem Internet ins LAN zeigt. Dasselbe gilt auch aus der DMZ ins LAN, wobei es hier auf die in der DMZ platzierten Applikationen ankommt.

6. Schreiben Sie sich nun die getroffenen Verbindungen auf ein A4 Blatt auf (Start, Ziel, Dienst).

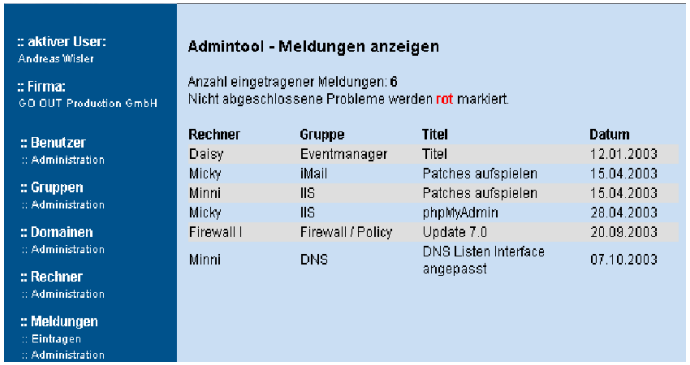
7. Mit diesem Blatt Papier können Sie sich nun an die Umsetzung in der Firewall machen.

5 Kontrolle

Sobald nun alle Verbindungen gemäss dem erstellten Konzept eingerichtet wurden, müssen Sie diese testen. Für die Arbeit gibt es im Internet eine Vielzahl von Tools, die einen so genannten Portscan durchführen. Sie testen alle Ports durch und geben an, wenn ein Port geöffnet ist. Vergleichen Sie diese Resultate mit Ihrem Konzept. Stimmen diese überein? Falls nicht, suchen Sie den Fehler in Ihrem Konzept und beheben Sie anschliessend den Fehler in Ihrer Firewall.



Version: 3.3, Shareware (30 Tage)
GFI Software Ltd., http://www.gfi.com/lannetscan/



6 Mutationen

Sehr schnell verändert sich die Infrastruktur. Ports werden geöffnet, andere werden geschlossen. Denken Sie an die Aktualisierung Ihres Konzeptes bzw. der Einstellungsliste. Bei einem Absturz der Firewall können Sie die Ports korrekt wieder einrichten. Ein Logbuch hilft Ihnen bei dieser Arbeit. Tragen Sie hier zusätzlich jede Veränderung ein. Die GO OUT Production GmbH bietet ein Tool an, mit welchem Sie diese Dokumentationsarbeit online erledigen können. Obenstehendes Bild zeigt Ihnen die Hauptmenu-Seite.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

7 Penetration Test

Nachdem das Konzept erstellt, die Firewall eingerichtet und die erste Kontrolle abgeschlossen sind, folgt ein Härtetest. Der so genannte Penetration Test, testet und reizt ihre Firewall und die dahinter, sichtbaren Applikationen.
Prüfen Sie die Verfügbarkeit, die Vertraulichkeit und die Integrität. Das bedeutet: die Simulation von DoS, Mailbombe, Mail Trojaner, Brute Force usw.

Für eine neutrale Beurteilung empfehlen wir Ihnen eine externe, auf Penetration Test spezialisierte, Firma zu beauftragen.

Die GO OUT Production GmbH prüft mit einem Penetration Test Ihre Firewall und die erreichbaren Dienste auf Herz und Nieren. Dabei werden die gefundenen Schwachstellen aufgespürt und dokumentiert. Anschliessend zeigen wir Ihnen, mit welchen Massnahmen die festgestellten Schwachstellen minimiert oder gar eliminiert werden können. Die maximale Zeit, die dafür aufgewendet werden darf, geben Sie vor.

Nach Abschluss des simulierten Hacker- oder Störangriffes, zeigen wir Ihnen das Resultat:

- Übersicht über die vom Internet erkennbaren Betriebssysteme, Dienste, Produkte und Versionen

- Im Falle von Sicherheitslücken:
- Risikoeinschätzung
- Massnahmenvorschläge
- Verbesserungen im Firewallkonzept oder der Architektur
- Know-How Transfer an der Schlussbesprechung

Ausführliche Informationen finden sie unter:
http://www.gosecurity.ch/penetration_test.asp

Nun ist Ihre Firewall auf die Gefährdungen aus dem Internet vorbereitet!

Haben Sie weitere Fragen? Wir stehen Ihnen gerne zur Verfügung. Sprechen Sie mit uns, vor es zu spät ist!