PROTECTSTAR

AWARD 2004

Computer Security

ZyXEL ZYWALL IDP 10

PROTECTSTAR
secure your business

Einleitung

Die Intrusion Detection and Prevention (IDP) Lösung, ZyWALL IDP 10 von ZyXEL, erkennt zuverlässig verschiedenste Attacken wie Würmer, Trojaner, Back-Door, Network- und Port-Scans, Buffer-Overflows und Anomalien und kann diese unerwünschten Kommunikationen unterbinden.

Die ZyWALL IDP 10 dient zum einen als interner Schutz hinter der Firewall (ermöglicht auch die Kontrolle von VPN-Verbindungs-Inhalten), wo sie gegen Würmer und internen Netzwerkangriffen schützt, oder sie kann vor einer Firewall (wobei auch die Firewall selbst zusätzlich geschützt wird) eingesetzt werden, wo sie den Internet-Verkehr auf potentielle Angriffe hin untersucht und Gegenmaßnahmen einleitet.

Die Appliance dichtet somit die letzten Lücken zwischen Internet und Intranet ab und lässt sich durch die einfache „Plug and Play"-Architektur innerhalb von Minuten in jedes Netzwerk integrieren.

Sicherheit

Im Gegensatz zu einer Firewall überprüft die ZyWALL IDP 10 in Echtzeit den Inhalt der Datenpakete auf über 1.600 Signaturen (im Test 1633 Signaturen). Ein Angriff löst sofort Alarm aus und leitet Abwehr-Maßnahmen ein.

Im regelmäßigen Update erhalten die Anwender aktuelle Regeln (Signaturen) die vor neuen Gefahren schützen. Dies bedeutet einen umfassenden Schutz für Unternehmen vor externen, als auch vor internen Angriffen und es wird zugleich ein Höchstmaß an Sicherheit gewährleistet. Die ZyWALL IDP 10 hat an den beiden Tagen unseres Testverfahrens alle zum Zeitpunkt bekannten 4834 verschiedenen Angriffs- und Sicherheitstest erfolgreich abgewehrt.

In diesen Testreihen wurden beispielsweise verschiedene Arten von Portscans, über zweihundert Denial of Service Angriffe, alle bekannten Schwachstellen von Firewalls und Betriebssystemen, sowie Sicherheitslücken in bestimmten Anwendungen, unter realen Bedingungen getestet.

Unseren vierstündigen Dauer-Penetrationstest hat die ZyWALL IDP 10 ebenfalls erfolgreich absolviert. Explizit zu nennen ist auch, dass die ZyWALL IDP 10 sowohl auf der Netzwerk- (Layer 3) als auch auf der Applikationsebene (Layer 7) effektiven Schutz bietet. Die ZyWALL 10 IDP kann so im „Inline"-, „Monitor"- und im „Bypass"- Mode (Device Operation State) betrieben werden. Bei dem „Inline Modus" ist die ZyWALL IDP 10 aktiv im Datenverkehr eingebunden. Der zu überwachende Datenstrom fließt durch das Gerät hindurch und wird anhand des Regelwerkes nach verdächtigen Angriffsmustern hin untersucht.

Das Intrusion Detection Modul alarmiert diese Angriffe und das Intrusion Prevention Modul blockt diese Datenströme sofort ab. Der ungefährliche Datenverkehr darf die ZyWALL IDP 10 ungehindert passieren. Das Intrusion Prevention bietet durch die Funktionalität des Auto-Prevention immer einen aktuellen Schutz, und schützt selbst vor neuen Würmern, lange bevor Signaturen für Antivirenprogramme zur Verfügung stehen.

Der Monitor Modus liest den gesamten Datenverkehr eines Netzwerkes mit.
So befindet sich die ZyWALL IDP 10 unsichtbar im Netz und beeinflusst somit auch nicht die Verfügbarkeit. Der so genannte „Flaschenhals" kann dadurch nicht entstehen. Als dritte Möglichkeit kann ZyWALL IDP 10 im „Bypass Modus" betrieben werden. In diesem Modus können alle Daten passieren und werden weder überprüft noch geloggt.

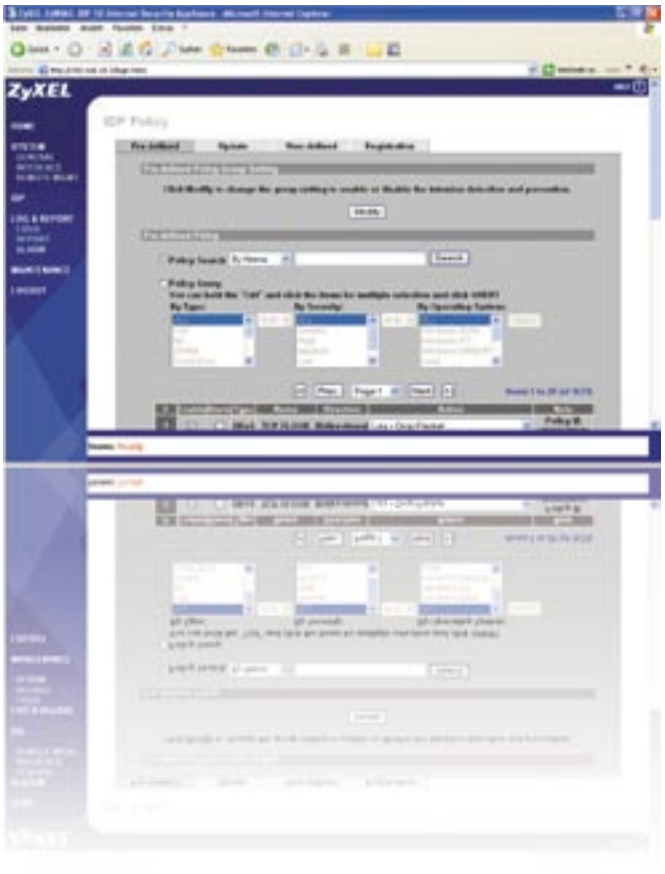
Durch jeweils einen Klick in der Konfiguration kann vom Bypass Modus (rein physikalische Einbindung) in den Monitor Modus (Intrusion Detection, keine Abwehrmassnahmen) und weiter in den Inline Modus (Intrusion Prevention) umgeschaltet werden. Es müssen also zum „Scharfschalten" des Systems nicht Unmengen von Regeln angepasst werden.

Im Gegensatz zu vielen anderen auf dem Markt erhältlichen IT-Sicherheitsprodukten analysiert die ZyWALL IDP 10 auch fragmentierte IP-Daten-Pakete. Der IP-Spoof-Schutz blockierte zuverlässig alle Nicht-Broadcast- und Multicast-Pakete, die an dem WAN-Port der Appliance eingehen und deren Quell-IP-

Adresse einem internen Teilnetz entsprach. Die Appliance sorgt zudem dafür, dass ein Firmennetzwerk vor Instant-Messaging-Services, Spam, Online-Spielen und Peer-to-Peer Missbrauch geschützt wird, da solche Applikationen nach Bedarf kontrolliert und unterbunden werden können.

Die Appliance kann momentan bis zu 3000 Signaturen verwalten, die sowohl Muster- als auch Anomalie-basiert arbeiten.
Die Anomalie-Erkennung der ZyWALL IDP 10 erkennt beispielsweise Abweichungen im Datenverkehr. Ein plötzliches Ansteigen der Datenmenge oder das völlige Lahmlegen eines Internetdienstes können auf einen Angriff hinweisen. Mit der Anomalie-Erkennung zeigt ZyWALL IDP 10 Abweichungen von definierten „normalen" Datenmengen an und meldet diese. Welche Datenmenge „normal" ist, kann die ZyWALL IDP 10 lernen und vom Administrator anpassen lassen. Ferner ist zu erwähnen, dass die ZyWALL IDP 10 keine Firewall ist, die offene Ports von Computersystemen versteckt oder blockiert, sondern

lediglich die gefährlichen Kommunikationen (auf Protokoll TCP und UDP) zu diesen Ports unterbindet. Dies ist der Grund dafür, dass



ein Angreifer bei einem gezielten Portscan auf sein Zielsystem - hinter der ZyWALL IDP 10 - dennoch offene Ports erfahren kann und dadurch Rückschlüsse auf aktivierte Dienste des Zielrechners ziehen kann. Sollten offene Ports von Systemen hinter der ZyWALL IDP 10 dennoch blockiert werden, so kann der Administrator manuell diese Ports von der Appliance sperren.

Allerdings ist zu beachten, dass die ZyWALL IDP 10 - wie bei allen anderen IDS-Systemen auch - nur IP-basierte Angriffe erkennen kann. IPX oder andere nicht-TCP/IP Ethernet Pakete können daher nicht von der Appliance untersucht werden.

Benutzerfreundlichkeit

Die Installation der ZyWALL IDP 10 ist anwenderfreundlich und der Installationswizard hilft dem Anwender das Gerät in wenigen Schritten zu konfigurieren und in Betrieb zu setzen. Jeder ZyWALL IDP 10 liegt eine CD-Rom bei, auf der sich das 111-seitige Handbuch als PDF-Datei befindet. Leider war das Benutzerhandbuch in unserem Test nur in englischer Sprache vorhanden. Zusätzlich ist ein 120-seitiger Quick Start Guide in gedruckter Fassung in sechs Sprachen (Deutsch, Englisch, Französisch, Spanisch, Italienisch und Chinesisch) enthalten.

Die Konfiguration der ZyWALL IDP 10 Appliance verläuft unproblematisch. Dennoch ist die individuelle Anpassung des Regelwerkes an ein bestehendes Firmennetzwerk nicht für unerfahrene Anwender oder Administratoren geeignet, auch wenn sich der Installationsaufwand durch vorkonfigurierte Sicherheitseinstellungen in Grenzen hält.

Um die Appliance in der Standard-Einstellung konfigurieren zu können, muss ein Computersystem an dem „Mgmt"-Port des Gerätes angeschlossen werden. Durch öffnen des Browsers und der Eingabe der IP-Adresse „192.168.1.3" (das Computersystem sollte eine IP-Adresse im gleichen Netzwerksegment haben bspw. 192.168.1.8) gelangt der Anwender zum Konfigurationsmenü der ZyWALL IDP 10, wo ihm ein entsprechender Installationswizard unterstützt. Das Default-Password lautet übrigens „1234".

Bei der Konfiguration kann der Anwender zunächst ein neues Zugangskennwort für die Konsole festlegen, dem Geräte eine neue IP-Adresse vergeben, die unterschiedlichen Policies bearbeiten und (de-)aktivieren, sowie den Verwendungszweck der Appliance (Inline-, Monitor-, Bypass-Modus) festlegen. Derzeit werden etwas über 1600 Intrusion Detection und Prevention Regeln von der ZyWALL IDP 10 unterstützt, die mit dem automatischen Software und Pattern Update ständig aktualisiert und erweitert werden. Bei den individuellen Einstellungen des Regelwerkes sollten dem Benutzer noch mehr Möglichkeiten zur Verfügung stehen, um das Gerät schneller an die Bedürfnisse eines Firmennetzwerkes anzupassen. Zusammenfassend können wir sagen, dass die ZyWALL IDP 10 in unseren Testreihen in knapp zwanzig Minuten konfiguriert und betriebsbereit war. Einmal vom Anwender konfiguriert, kann das Gerät sprichwörtlich vergessen werden, da kein Administrationsaufwand oder Wartungen mehr nötig sind.

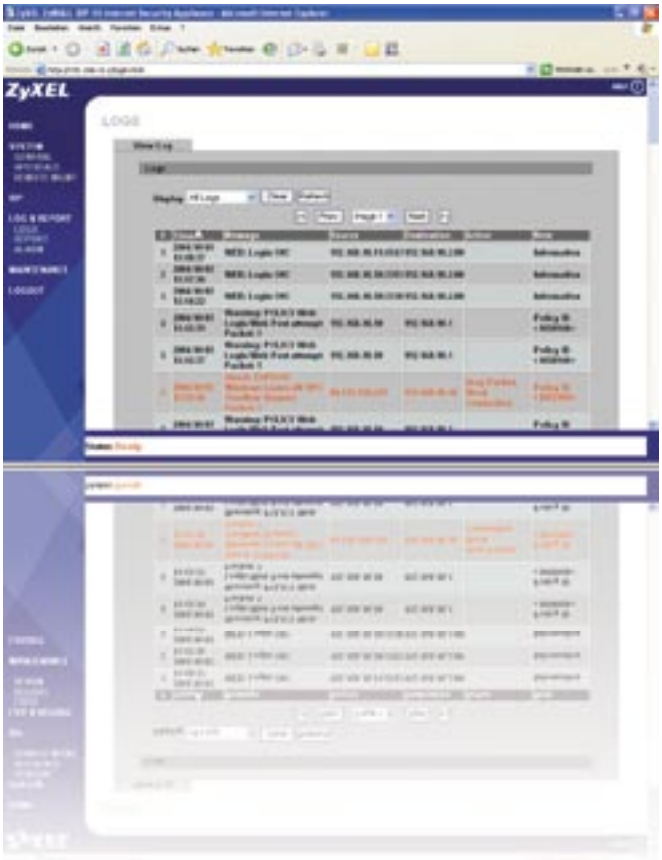
Performance

Die ZyWALL IDP 10 arbeitete bei unseren Testreihen schnell und zuverlässig.
Ein Durchsatz von 26 MBit/s bei üblichem Traffic und unter idealen Bedingungen sogar von bis zu 38 MBit/s, sowie eine Unterstützung von 8000 gleichzeitigen Verbindungen, sorgen für ausreichend Performance. Diese Leistung reicht, um ein kleines- oder sogar mittelständisches Unternehmen (Herstellerangabe: maximal 200 PC-Arbeitsplätze) mit seinen Mitarbeitern vor externen und internen Angriffen abzusichern.

Selbst während unseres vierstündigen Dauer-Penetrationstest konnte, unter minimalen Leistungseinbußen, mit der Appliance weiterhin gearbeitet werden.
Um die Performance der ZyWALL IDP 10 zu steigern, kann das Regelwerk so konfiguriert werden, dass nur diejenigen Regeln (bspw. Regeln für Windows XP, Solaris, Linux, etc.) aktiviert werden, für die Angriffe auf das Firmennetzwerk gefährliche Auswirkungen haben könnten.

Support

Mit dem Erwerb einer ZyWALL IDP 10 erhält der Anwender für ein Jahr lang die notwendigen Signaturen-Updates inklusive. Für jedes weitere Jahr fallen dann 18 Prozent des Anschaffungspreises an. Um die automatische Updatefunktion nutzen zu können, müssen sich Benutzer der ZyWALL IDP 10 unter HYPERLINK „http://www.myzyxel.com" www.myzyxel.com registrieren. Jeder ZyWALL IDP 10 liegt ein Aktivierungskey bei, mit dem dann das 1-Jahres-Update freigeschaltet werden kann. Außerdem kann dort der „Threat Thermometer" eingesehen werden, der Informationen über aktuelle Sicherheitslücken und im Umlauf aktive Würmer und Gefahren bereithält.



Zudem können deutsche Anwender unter HYPERLINK „http://www.zyxel.de“ www.zyxel.de auf eine umfangreiche Wissensdatenbank (Knowledgebase) und einem Download-Bereich zugreifen, wo die aktuellen Dateien oder das Handbuch heruntergeladen, sowie die am häufigsten gestellten Fragen (FAQ) betrachtet werden können. Ebenfalls über diese Webseiten kann der Anwender eine Supportanfrage über ein vorgefertigtes Online-Formular stellen.

Preis / Leistung

ZyWALL IDP 10 bietet einen hervorragenden und aktiven Echtzeit-Schutz zu einem bisher am Markt nicht bekannten Preis-/Leistungsverhältnis. Mit einem empfohlenen Verkaufspreis von 2.298 Euro (brutto) ist die ZyWALL IDP 10 ein echter Geheimtipp und zugleich eines der preiswertesten IDS/IDP-Lösungen auf dem IT-Sicherheitsmarkt. Andere Hersteller verlangen hier oftmals zwischen 5.000–20.000 Euro.

Zudem ist zu erwähnen, dass die Anzahl der zu schützenden Systeme für die Lizenzierung nicht relevant ist und keine weiteren Kosten entstehen, unabhängig davon ob der Anwender nun zwei oder zweihundert Systeme mit der ZyWALL IDP 10 absichern möchte.

Fazit

Die ZyWALL IDP 10 zur Intrusion Detection and Prevention stellt die erste Sicherheitslösung in einer neuen und zukunftsweisenden Generation von ZyXEL Security Produkten dar. Die Appliance ist speziell für kleine und mittelständische Unternehmen entwickelt worden, die ein solides und kosteneffektives System zur Erkennung und zum Schutz vor Eindringlingen suchen. So knüpft die Appliance dort nahtlos an, wo Antiviren-Scanner und Firewalls mit ihren Sicherheitsmechanismen aufhören und schützt Unternehmen sowohl vor bösartigen externen als auch vor internen Angriffen auf der Netzwerk- und Anwendungsebene, und das zu einem günstigen Preis.

Die Signaturendatenbanken mit derzeit 1633 Regeln bieten einen ausreichenden Schutz. Dennoch sollten sie nachhaltig erweitert werden. Zudem sollte ein Zugang zur WEB-Konfigurationskonsole über den verschlüsselten Port 443 (HTTPS) der ZyWALL IDP 10 hinzugefügt werden und die individuelle Einstellung des Regelwerkes etwas erleichtert werden. Wir empfehlen kleinen Unternehmen die ZyWALL IDP 10 hinter einer Firewall zu postieren. Am besten in Kombination mit einer ZyXEL-Firewall (ZyWALL 70 oder ZyWALL 35).

Größere Unternehmen sollten sowohl hinter einer bestehenden Firewall eine oder nach Bedarf mehrere ZyWALLs IDP 10 postieren, als auch in unternehmenskritischen Netzwerkbereichen (Beispiel: zwischen LAN-Segmenten oder zwischen LAN und WLAN), wo interne Daten vor ungewollten Zugriffen geschützt werden sollen.

Die Appliance ZyWALL IDP 10 von ZyXEL erhält aufgrund der sehr guten Testergebnisse und den vielseitigen Einsatzmöglichkeiten den „ProtectStar-AWARD“ für das Jahr 2004.

www.ProtectStar.com

Impressum:

PROTECTSTAR
secure your business

ProtectStar Inc.
Testcenter

Postfach 10 25 08
D-86015 Augusburg
Germany

www.protectstar.com
testcenter@protectstar.com

Gestaltung und Konzeption:

wo-pro werbung

wo-pro werbung -agentur für klassische und neue medien
Wettringer Str. 32
D-74585 Kleinansbach

Fon: 07958 92 57 14
Fax: 07958 92 68 98
E-Mail: info@wo-pro.de
Web: www.wo-pro.de