

4 Defense

Die Abwehr gegen Hackerangriffe mittels technologischen Mitteln ist in jedem Fall sinnvoll. Welche Massnahmen man jedoch ergreifen sollte, richtet sich in erster Linie nach dem Wert der vorhandenen Daten, die zu schützen sind. Als Grundlage jeder Abwehrstrategie steht ein funktionierendes Backup-Konzept.

4.1 Professionelle Firewall mit VPN und Vlan

Nebst einem Backup ist eine professionelle Firewall Pflicht. Wir setzen die OpenSource basierte pfSense ein, die auf FreeBSD aufbaut. Nebst den Firewall-Regeln bietet pfSense auch Routerfunktionalität wie DHCP, Vlan oder IPv6 und bietet zudem VPN (IPsec, L2TP oder OpenVPN sowie WireGuard). pfSense bietet ein Web-Management sowie ein SSH-Zugang und lässt sich auf verschiedener Hardware ausführen.



4.2 Monitoring

Insbesondere bei grösseren Netzwerken bietet sich eine Überwachung der Netzwerkgeräte an. So lassen sich Ausfälle oder untypisches Verhalten schnell erkennen. Dazu eignet sich z.B. Nagios oder das OpenSource basierte Icinga.

Nagios[®] Current Network Status
 Last Updated: Fri Apr 28 20:24:50 CEST 2017
 Updated every 90 seconds
 Nagios® Core™ 4.3.1 - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals
 Up: 3, Down: 0, Unreachable: 0, Pending: 0
 All Problems: 0, All Types: 3

Service Status Totals
 OK: 17, Warning: 0, Unknown: 0, Critical: 0, Pending: 0
 All Problems: 0, All Types: 17

Service Status Details For All Hosts

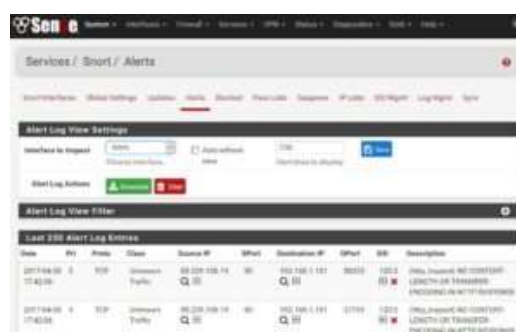
Host	Service	Status	Last Check	Duration	Attempt	Status Information
hpe1920	PING	OK	04-28-2017 20:22:31	1d 3h 27m 19s	1/3	PING OK - Packet loss = 0%, RTA = 1.47 ms
	Port 1 Link Status	OK	04-28-2017 20:22:35	1d 1h 52m 15s	1/3	SNMP OK - 1
	Uptime	OK	04-28-2017 20:17:15	1d 1h 57m 35s	1/3	SNMP OK - 1823752934
localhost	Current Load	OK	04-28-2017 20:23:19	9d 7h 56m 17s	1/4	OK - load average: 0.40, 0.68, 0.85
	Current Users	OK	04-28-2017 20:24:24	9d 7h 55m 39s	1/4	USERS OK - 0 users currently logged in
	HTTP	OK	04-28-2017 20:20:29	9d 7h 55m 2s	1/4	HTTP OK: HTTP/1.1 200 OK - 10975 bytes in 0.001 second response time
	PING	OK	04-28-2017 20:19:44	9d 7h 54m 24s	1/4	PING OK - Packet loss = 0%, RTA = 0.09 ms
	Root Partition	OK	04-28-2017 20:24:13	9d 7h 53m 47s	1/4	DISK OK - free space: / 96412 MB (94% inode=98%):
	SSH	OK	04-28-2017 20:21:43	9d 7h 53m 9s	1/4	SSH OK - OpenSSH_6.7p1 Debian-5+deb8u3 (protocol 2.0)
	Swap Usage	OK	04-28-2017 20:22:18	9d 7h 52m 32s	1/4	SWAP OK - 100% free (4670 MB out of 4676 MB)
pfsense	Total Processes	OK	04-28-2017 20:22:57	9d 7h 51m 54s	1/4	PROCS OK: 91 processes with STATE = RSZDT
	CPU Load	OK	04-28-2017 20:20:59	0d 21h 3m 51s	1/3	OK - load average: 0.00, 0.02, 0.00
	Current Disk Space	OK	04-28-2017 20:20:31	0d 20h 44m 19s	1/3	DISK OK - free space: / 1544 MB (66% inode=95%):
	Current Users	OK	04-28-2017 20:15:02	0d 20h 59m 48s	1/3	USERS OK - 1 users currently logged in
	Current Varrun	OK	04-28-2017 20:21:49	0d 20h 43m 1s	1/3	DISK OK - free space: /var/run 3 MB (96% inode=95%):
pfsense	Current Zombie Procs	OK	04-28-2017 20:23:07	0d 20h 41m 43s	1/3	PROCS OK: 0 processes with STATE = Z
	Total Processes	OK	04-28-2017 20:24:25	0d 20h 40m 25s	1/3	PROCS OK: 62 processes

Results 1 - 17 of 17 Matching Services



4.3 Intrusion Detection

Durchaus kann auch eine laufende Überwachung des Netzwerkverkehrs sinnvoll sein. Ein solches Intrusion Detection System arbeitet viel zuverlässiger als ein herkömmliches Antivirenprogramm. Eine bekannte Software ist Snort. Snort lässt sich als Package auf der pfSense Firewall integrieren. Snort ist aber nicht nur für FreeBSD erhältlich sondern auch für Linux-Distributionen und Windows. Es ist auch so, dass SNORT nicht zwangsweise auf der Firewall laufen muss. Mittels Port Mirroring kann man den Netzwerk Traffic auf einen beliebigen Überwachungsserver leiten.



Im Bereich der Überwachung des Internetverkehrs gibt es noch weitere Ansatzpunkte. pfBlocker blockiert Webseiten anhand einer Blacklist. Für grössere Firmen ist eine professionelle Lösung von Suricata auf der pfSense erhältlich.

5 Notfall-Hilfe

Im Notfall entfernen wir Viren, Trojaner und Spyware von Ihrem EDV System. Dabei hat die Sicherheit der Geschäfts-Daten sowie die Wiederherstellung eines sauberen Systems Vorrang.

Im Normalfall ist das Booten einer Linux CD wie Ct'Desinfect die beste Lösung, um einen befallenen Computer zu reinigen. Im Spezialfall kann es jedoch sinnvoll sein, die Harddisk auszubauen und so zu untersuchen.

