4 Defense

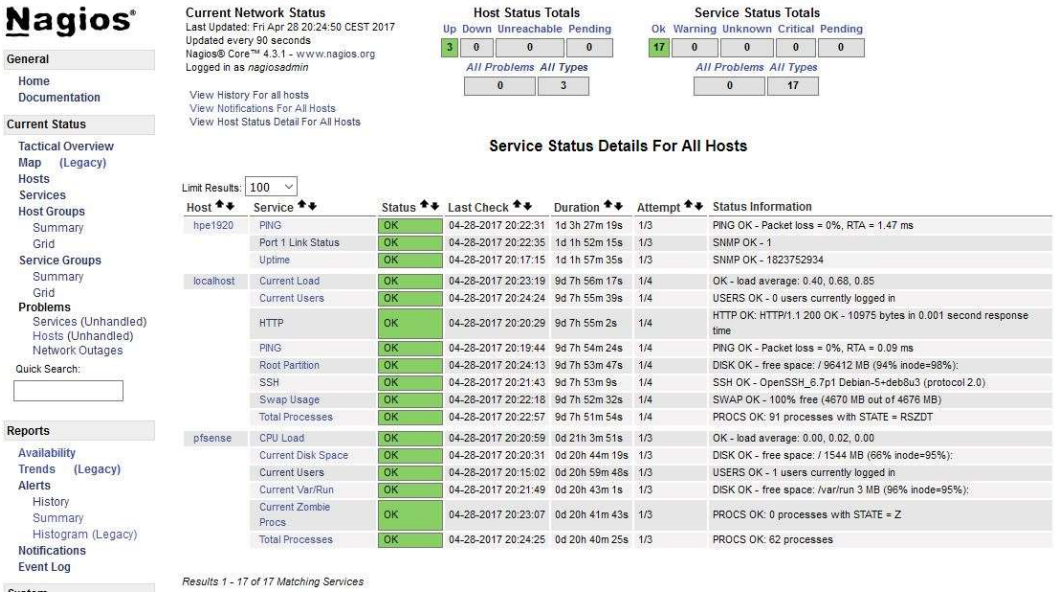
Die Abwehr gegen Hackerangriffe mittels technologischen Mitteln ist in jedem Fall sinnvoll. Welche Massnahmen man jedoch ergreifen sollte, richtet sich in erster Linie nach dem Wert der vorhandenen Daten, die zu schützen sind. Als Grundlage jeder Abwehrstrategie steht ein funktionierendes Backup-Konzept.

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.



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 Antivirenprogram. 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.