Welcome to

Managed Security Services og Entrepreneurship

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

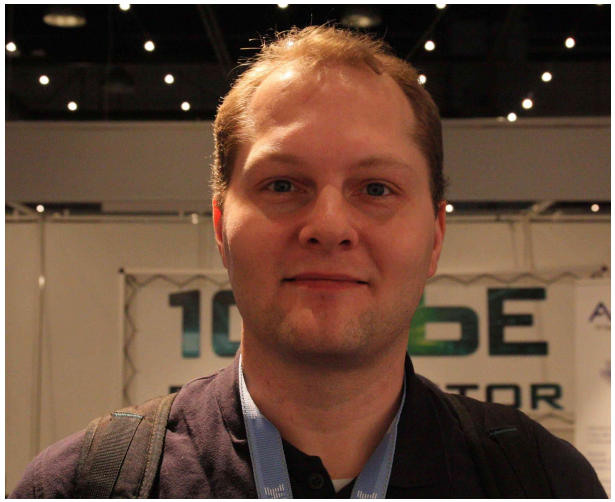
http://www.solidonetworks.com

Tema

Dagens tema

Temaet er Managed Security Services samt it-projekters interaktion med informationssikkerhed i virksomheder.

Kontaktinformation og profil



- Henrik Lund Kramshøj, IT-sikkerhed og internet samurai
- Email: hlk@solido.net Mobil: +45 2026 6000
- Cand.scient fra Datalogisk Institut ved Københavns Universitet, DIKU
- CISSP certificeret
- 2003 - 2010 Selvstændig sikkerhedskonsulent
- 2010 Stifter og partner i Solido Networks ApS

The early years 1980'erne

Vores branche er jo meget ung

Der var mainframes, men alt andet var hjemmecomputere

C= 128, CP/M, Floppy disk - der kunne bøjes

Intel 386! Windows 3.0!

Viden om computere var blandt nørder

Internet, .com bølgen 1990'erne

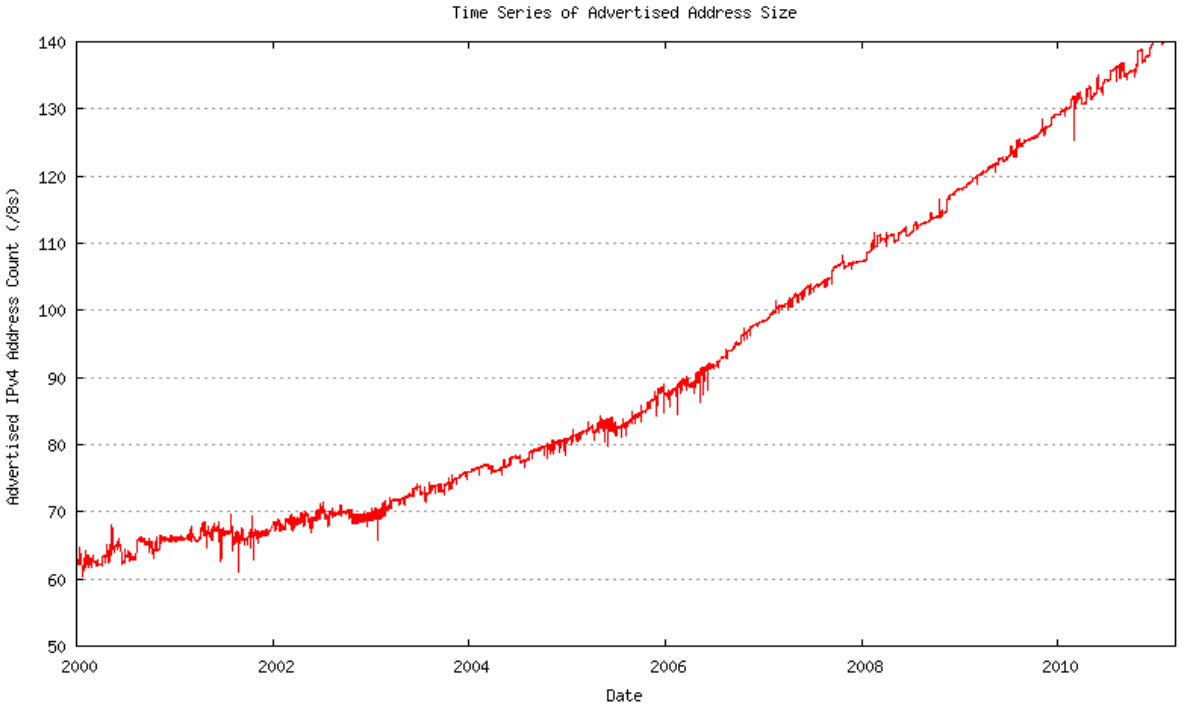
SOLIDO NETWORKS

> The commercialization of what was by the 1990s an international network resulted in its popularization and incorporation into virtually every aspect of modern human life. As of 2009, an estimated quarter of Earth's population used the services of the Internet.
>
> ...
>
> On 6 August 1991, CERN, a pan-European organization for particle research, publicized the new World Wide Web project. The Web was invented by British scientist Tim Berners-Lee in 1989.

Kilde: `http://en.wikipedia.org/wiki/Internet`

Jeg startede på DIKU efteråret 1990 ☺

Modningsprocessen 2000s



IPv4 Address Report

The next data set is total span of address space advertised in the BGP routing table over time. The data has been collected on a 2-hourly basis since late 1999.

Kilde: `http://www.potaroo.net/tools/ipv4/`

Idag - the network IS the computer

Buzzword bingo: Cloud, XML, SOAP, REST, XML

Platform as a Service (PaaS) is the delivery of a computing platform and solution stack as a service.

Software as a service (SaaS)

Høj kompleksitet $=>$ computing er på linie med vand, el, gas

Er det en computer hvis den ikke har internet?

Fremtiden - 2010 og fremefter

The Mobile Network in 2010 and 2011

Global mobile data traffic grew 2.6-fold in 2010, nearly tripling for the third year in a row. The 2010 mobile data traffic growth rate was higher than anticipated. Last year's forecast projected that the growth rate would be 149 percent. This year's estimate is that global mobile data traffic grew 159 percent in 2010.

...

Last year's mobile data traffic was three times the size of the entire global Internet in 2000. Global mobile data traffic in 2010 (237 petabytes per month) was over three times greater than the total global Internet traffic in 2000 (75 petabytes per month).

...

There will be 788 million mobile-only Internet users by 2015. The mobile-only Internet population will grow 56-fold from 14 million at the end of 2010 to 788 million by the end of 2015.

Kilde: *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010 - 2015*

Security6.net

Security, IPv6, Networking and Unix

Startdato ca. januar 2003

Enkeltmandsvirksomhed, indtil 2010

Ingen managed security services

Security6.net profile

Kunder

Mellemstore til store firmaer, kun erhvervskunder

Medicinalvirksomheder, hostingfirmaer, offentlige instanser,

Opgaver

Sikkerhedsanalyser, audit, aktive hacker test/pentest

Undervisning, Linux, Unix, TCP/IP, netværk, switche, firewalls, computer forensics

Konsulentarbejde indenfor internetteknologier, infrastruktur, firewalls, VPN, ...

Arbejdsområde: nationalt og internationalt

En ansat

Managed security giver mening!

Trenden går mod komplekse infrastrukturer, mere af den og højere krav

Kunderne vil have høj oppetid, fordi internet teknologier er forretningskritiske

Kunder der ikke betragter netværket som forretningskritisk lider tab

Kunderne har ikke *nok* netværk til at have fuldtidsansatte

Hvad skal der til for at tilbyde Managed Security Services

Typiske Managed Security Services

SOLIDO NETWORKS

> In computing, managed security services (MSS) are network security services that have been outsourced to a service provider.

Kilde: `http://en.wikipedia.org/wiki/Managed_security_service`

Opgaver som tidligere blev håndteret in-house, eller ignoreret:

Event opsamling og analyse, Email scanning, Anti-virus og spam,

Firewall opsætning, drift og konfiguration

Netværksopsætning internt, STP, RSTP, stacks, LACP, LLDP, ...

Netværksopsætning eksternt, BGP, LC-SC, single-mode, mono-mode, multi-mode, link-net, PI, PA, RIPE

Angreb DoS, DDoS m.v.

Angreb anno 2009

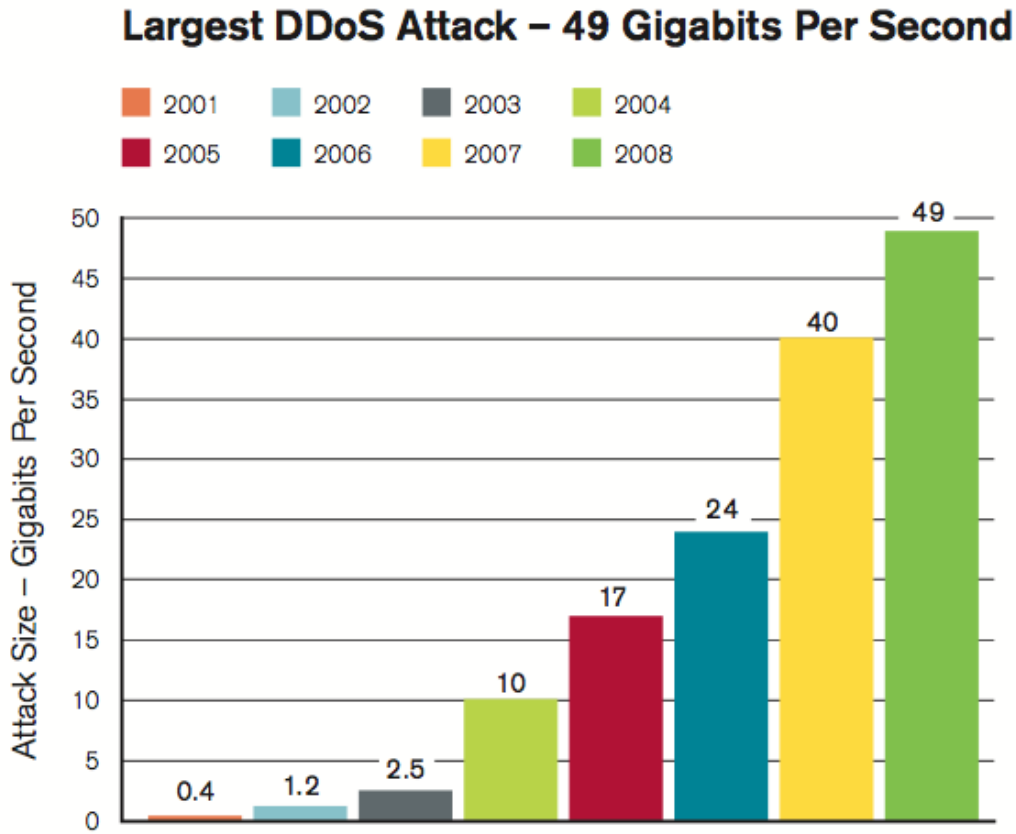


Figure 1: *Largest DDoS Attack – 49 Gigabits Per Second*

Source: Arbor Networks, Inc.

Kilde: Arbornetworks: Worldwide Infrastructure Security Report 2009 Report

Angreb anno 2010

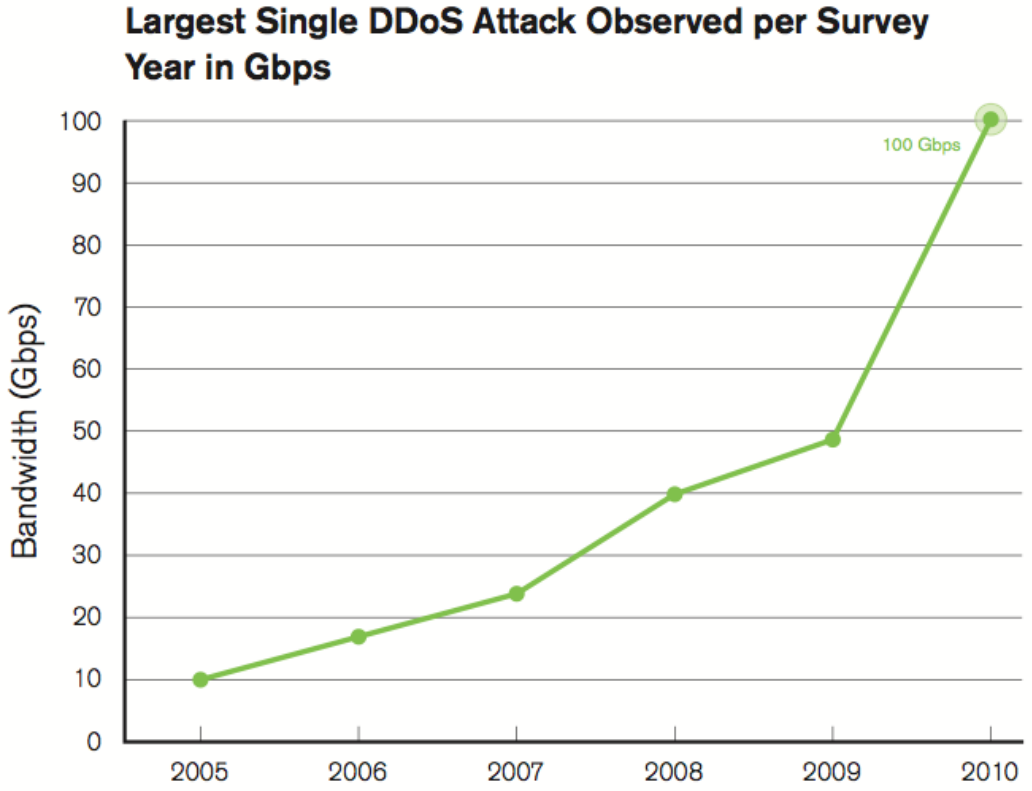


Figure 1
Source: Arbor Networks, Inc.

Kilde: Arbornetworks: Worldwide Infrastructure Security Report 2010 Report

Vejen som leverandør

Secure Hosted firewall

The Secure Hosted Firewall solution protects your servers from internet attacks while allowing your customers to access your services. This product relieves you from the burden of selecting, installing and running your own firewalls in front of your servers.

Solido Networks will configure access from your requirements and will take care of everything else.

Vi ser et behov for managed services

IT-afdelingen hverken kan eller skal være eksperter i alt

Vi prøver at definere produkter, som er nemme at vælge til og fra

Solido Networks anno 2010

Security6.net kunne ikke tilbyde MSS

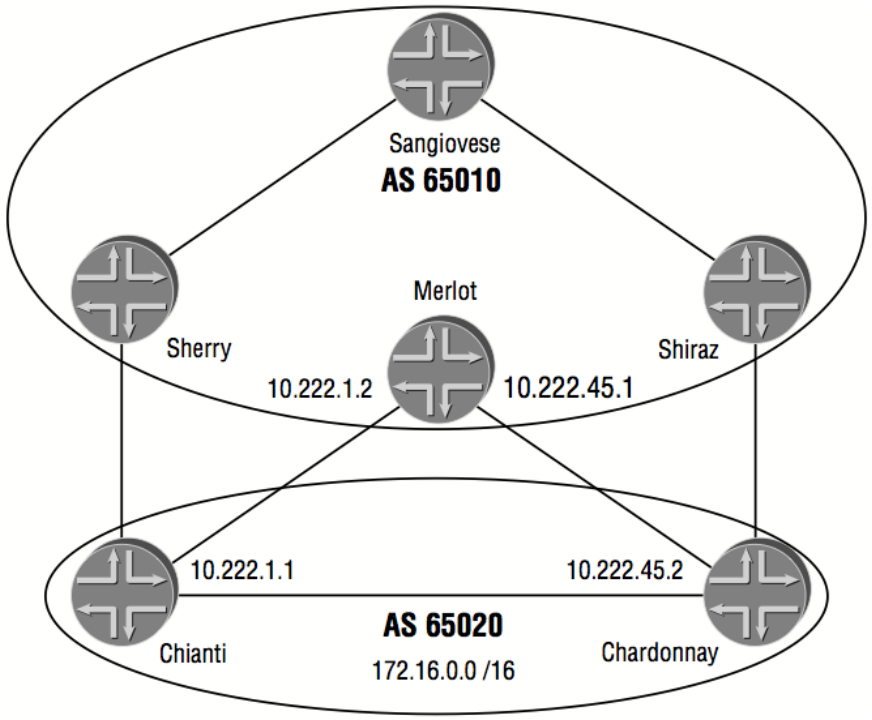
Vi fandt en partner i Solido Hosting, Christer Hasse

Security6.net medbragte viden om sikkerhed og netværk, kunder

Solido Networks fik viden om drift, kapacitet, størrelse, kunder fra Hosting

Solido Networks filosofi

FIGURE 4.17 BGP sample network



Vær eksperter indenfor vore kerneområder - internet, infrastrukturer og sikkerhed

Lav et fleksibelt produkt og sæt prisen derefter, skalerbart

Services vi tilbyder

Managed firewall - filtrering af 10Gbit internetforbindelser

Managed netværk, BGP, PI ansøgninger, routing protokoller, VPN, SSL VPN, IPv6

Få en fiberforbindelse med det hele, filtrering, remote backup, VPN, routing - alt inklusiv

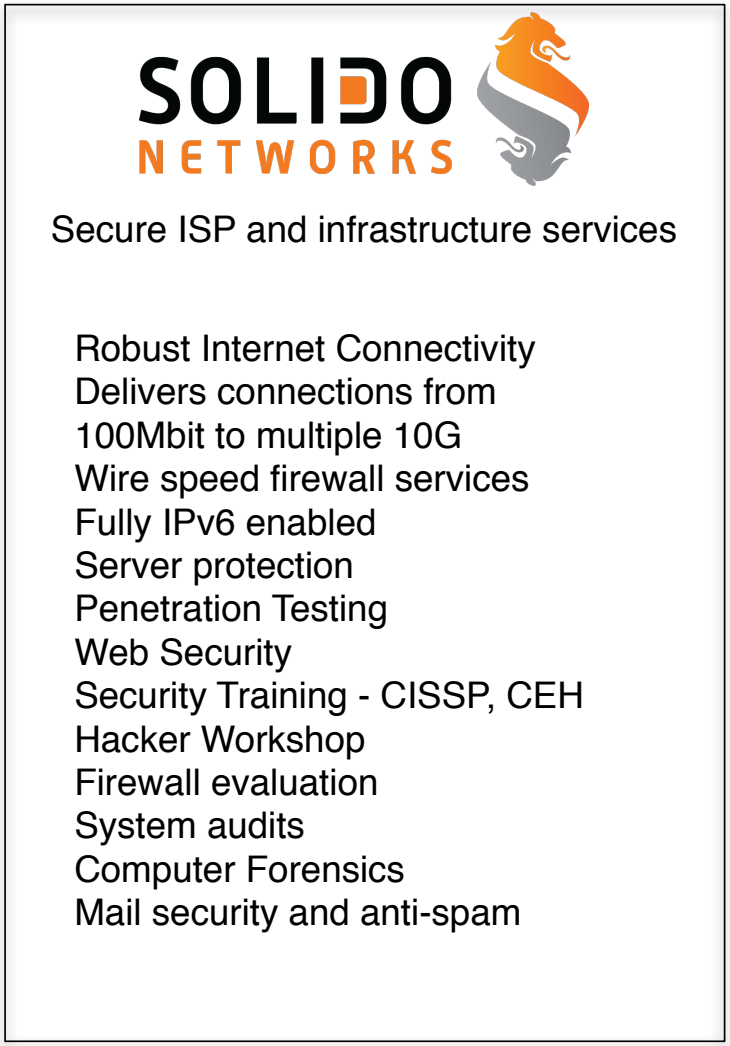
Audit af netværk løbende, som en service - aktive pentest, paper review

Mange af vores services kræver at vi har meget kapacitet

Høj kapacitet som er dårligt udnyttet er dyr

Ting som kun udføres een gang eller sjældent hos kunderne

Oversigten



Værdien for kunderne

	SRX100	SRX210	SRX220	SRX240
JUNOS Software version tested	JUNOS 10.3	JUNOS 10.3	JUNOS 10.3	JUNOS 10.3
Firewall performance (max)	650 Mbps	750 Mbps	950 Mbps	1.5 Gbps
IPS performance (NSS 4.2.1)	60 Mbps	80 Mbps	100 Mbps	250 Mbps
AES256+SHA-1 / 3DES+SHA-1 VPN performance	65 Mbps	75 Mbps	100 Mbps	250 Mbps

Kunderne af idag kender problemerne:

Netværksenhederne er dyre

Køb den lille og den er for lille - snart

Administration, overvågning, drift - hvad er kerneforretningen?

Go big, or go home

SRX240	SRX650	SRX1400	SRX3400
JUNOS 10.3	JUNOS 10.3	Junos 10.4	Junos 10.2
1.5 Gbps	7 Gbps	10 Gbps	20 Gbps
250 Mbps	900 Mbps	2 Gbps	6 Gbps
250 Mbps	1.5 Gbps	2 Gbps	6 Gbps

Vores kerneforretning er at drive det bedste og sikreste netværk

Udfordringerne i MSS

Definition af nye produkter - hvad får kunden

Kommunikation, både ved ændringer, problemer, opfølgning

Det er en omstilling for os at definere produkterne, men sundt

Kunderne er ikke vant til at overlade så meget til os

Hvem har reelt kontrollen? kan man out-source sikkerhed?

Ansvar - SLA dækker jo oppetid, hvad med brud på sikkerheden

Virtualisering af sikkerhed

Opsummering

Solido Networks er et nyt firma og vi lærer hele tiden

Vi vokser støt og roligt

Har idag 3*10Gbit internetforbindelser i Ballerup, Interxion

Har idag et bredt udvalg af services indenfor netværk og sikkerhed

Spørgsmål?

SOLIDO NETWORKS

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

I er altid velkomne til at sende spørgsmål på e-mail

Reklamer: kursusafholdelse

Følgende kurser afholdes med mig som underviser

- IPv6 workshop - 2 dage
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 1-2 dage
  En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og wirksomhedsnetværk.
- Hacker workshop 2 dage
  Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, OpenVAS m.fl.
- Forensics workshop 2 dage
  Med fokus på tilgængelige open source værktøjer gennemgås metoder og praksis af undersøgelse af diskimages og spor på computer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage
  Informere om trusler og aktivitet på Internet, samt give et bud på hvorledes en avanceret moderne firewall idag kunne konfigureres.

Se mere på `http://www.solidonetworks.com`