ErgoGroup - a leading Nordic IT company:

www.ergogroup.no

How we organize security – nothing very original here:

Several lines of defense – e. g.:

Anti virus software on servers and clients

Organized patch management

Filtering on web proxies

Extensive use of firewalls

Network based IDS (NIDS) is just a small part of this.

The service is outsourced to an external firm

It needs continuous manning by trained , highly competent analysts at the IDS firm. Therefore the cost is relatively high

My role:
Receive event warnings, analyze them and track nodes, mainly based on IP-addresses. Has worked nearly ten years in this field.

I formulate warnings to those cleaning up – administrators of clients and servers etc. based on event reports from the provider.

This role is necessary because the external firm cannot have full overview over our solutions and organization.

Technical details:

The network traffic is sniffed via a tap at the periphery

Sniffed traffic (a copy) is distributed by a specialized switch to several sensors

The sensors are simple servers - Linux, BSD or appliance (which has a Linux or BSD base also)

Gigabyte capacity is necessary

Discovery is signature based

Much in common with a virus scanner

This means that 0-day exploits might pass by undiscovered

Many attacks have common signatures however, so some new attacks are discovered

Anomaly based, statistical methods are a distant dream

The latter is much written about in research papers, but signature based methods dominate in practice

What we see of attacks

Almost all are blind in the sense that the attackers do not know and do not care what kind of firm or organization the attacked nodes are in

The motive the last years seem to be to build botnets which are used for spam and possibly other criminal activities not related to the site of the attacked nodes. Sometimes also to swindle the user.

The last year has more and more been dominated by attempts at fake antivirus installation

Worm attacks have been rare, with Conficker as a notable exception

Besides we stop various kinds of policy violations by employees - file sharing, gaming etc.

Attack examples

Buffer overflows of widespread software, now third party software (e.g. Adobe Acrobat) more than Microsoft products

Social engineering in order to fool users into downloading becomes more and more important

Attacks are mostly directed at Microsoft clients and servers.

We see some bruteforce password guessing attacks on Linux units

False positives

In my view over focused in research papers. Irrelevant or insignificant attacks are almost as important

Must be defined in the context they are observed.

Said to be a major problem with anomaly based methods

After several years of cooperation with the IDS provider, a small problem for us

And of course: False negatives are the REAL problem

What do we achieve?

IDS said to be "script kiddy" detection - to day: petty crime detection

The really dangerous attacks, "spear fishing" etc. will probably creep under the radar in most cases

In my view the important thing is to build a security culture by keeping watch

- and I think that if the users know we keep watch they will be observant too