GigaCampus institusjonsgjennomgang, sikkerhet

Institusjon: NN
Studiested: NN
Dato: xx.xx.xxxx
Deltakere: NN fra NN.
NN fra UNINETT.

Omfang

Gjennomgangen ble inndelt i følgende fire hoveddeler:

- Generelt
- Sikkerhet i endesystemer
- Sikkerhetsfremmende nettdesign
- Lokal sikkerhetsovervåkning

Gjennomgangen ble foretatt med utgangspunkt i en sjekkliste med detaljerte punkter innen hver hoveddel.

Bakgrunnen for gjennomgangen er å skaffe en oversikt over hvordan det står til med sikkerhetsarbeidet i sektoren med tanke på utarbeidelse av felles beste praksis gjennom GigaCampus-arbeidsgruppene.

Sammendrag

-

Anbefalinger

-

Rapporten

Denne rapporten har form av en utfylt sjekkliste, der resultater og merknader fra alle punktene innen samtlige hoveddeler er gjengitt.

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

Generelt

Omfang: Post 0, 1 og 2.

Post nr	Sjekkpunkt	Merknader
0.0	**Om institusjonen**	
0.1	- Antall studenter/ansatte/maskiner - Studiested(er) - Studieretninger	

Post nr	Sjekkpunkt	Merknader
1.0	**Sikkerhetspolicy (SP)**	
1.1	Gjennomføring og planer - Status for arbeidet? - I tilfelle ikke påbegynt, foreligger det planer?	
1.2	Risiko- og sårbarhetsanalyse (ROS) - Er noe slikt gjennomført, og i så fall i hvilken form?	
1.3	Forankring - Er SP (og ev. ROS) forankret i toppledelsen? - Er det utarbeidet rutiner/handlingsplaner for sikkerhetsarbeidet? Koblet mot SP?	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

1.4	Brukeradferd og IT-reglement - Finnes det et IT-reglement? Hva inneholder dette? Reaksjoner? - Hvem skal få gjøre hva og hvor? - På en skala fra 1 til 10 (1=min, 10=maks): - Hvor strengt mener dere at deres IT-reglement er? - Hvor strengt mener dere det burde vært? - I hvilken grad mener dere at dere klarer å håndheve det? - Har dere inntrykk av at brukerne har forståelse for hvorfor IT-reglementet er som det er? - Er en eventuell motvilje en trussel i seg selv? - Omtaler IT-reglementet institusjonens erstatningsansvar overfor brukere (f.eks. ved tap av data)? - Går det frem av IT-reglementet hvorvidt studenter og ansatte selv er ansvarlige for sine handlinger?	
1.5	Personvern – Hvordan håndteres informasjon som er sensitiv mht personopplysninger? – Finnes det dokumenterte rutiner for å håndtere slik informasjon?	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

Post nr	Sjekkpunkt	Merknader
2.0	**Sikkerhetsteam og abusehåndtering**	
2.1	Personell - Folk med definert sikkerhetsansvar? - Bakgrunnsjekk / Taushetserklæring? - Organisering / Ressurser? - Tilgjengelige ressurser i et typisk døgn? - Eksisterer det noen vaktordning? - Veldefinerte kontaktpunkt for henvendelser? - Eksisterer abuse-adresse? Blir den lest, og av hvor mange? - Støtte for e-postkryptering (PGP e.l.)?	
2.2	Kompetansepåfyll - Får man bygd opp kompetanse? - Fra hvor? Egen lesing?	
2.3	Katastrofehåndtering - Organisering - Rutiner	
2.4	Ansvar og myndighet - Er funksjonen forankret i toppledelsen? - Hva slags myndighet har sikkerhetspersonell?	

2.5	Sikkerhetshendelser - Hvordan oppdages hendelser? - Føres det oversikt over hendelser? - Rutiner for håndtering av hendelser? - Sikring av bevismateriale, analyse ... - Utlevering av materiale? Anonymisering? - Reetablering? - Eskalering av hendelser? - Foretas det evaluering etter hendelser?	
2.6	Copyright-problematikk - Føres det oversikt over hendelser?	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

Sikkerhet i endesystemer

Omfang: Post 3 og 4.

Post nr	Sjekkpunkt	Merknader
3.0	**Operativsystem og basis programvare**	
3.1	Standardinstallasjoner - Administratorbrukere/grupper - Delt administrator-konto? - Personlige kontoer med utvidede privilegier? - Tjenestespekter - «Vanilla» eller modifisert? - Metoder for fjernaksess? - Til hvilke maskiner? - Forskjell på ansatt- og studentmaskiner? Andre klasser?	
3.2	Standard applikasjonsportefølje(r) - Opereres det med noe slikt? - Håndteres dette sentralt (på tjener), lokalt (på klient) eller begge deler? - Håndtering av avvik?	

3.3	Livssyklus - Sentralt verktøy for konfigurasjon/patching? - Testing av patcher? - Rutiner - Ulike OS - Ghosting og sentrale image? - Gamle installasjoner - Embedded / sær hardware/software - Sanering av utstyr brukt ifm. prosjekter/lab?	
3.4	Skanning og integritetskontroll - Kontroll på hva som kjører hvor? - Tjenester som tilbys? - Gjøres det integritetskontroll av systemfiler på sentrale system? - Rutiner?	
3.5	Logging - Sentral logg-server? - Bruk av loggmateriale. Reaktivt? Proaktivt? - Forvaltning av loggmateriale?	
3.6	Studenthybler - Juridiske forhold, myndighet/ansvar? - Anbefalinger/krav til studentene og maskinvare/programvare?	

3.7	Bruker- og passordhåndtering - Oppfølging fra «fødsel» til «død»? - Endring av privilegier? - Brukerdatabaser, systemer med egne regimer? - Gjestekontoer? - Avlyttingsfare, passord i klartekst?	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

Post nr	Sjekkpunkt	Merknader
4.0	**Sikkerhetsfremmende tilleggsprodukter**	
4.1	Antivirus-programvare - Rutiner? - Hvem har tilbud om produktet? - Konfigurering? - Anbefalinger?	
4.2	Lokale brannmurer - Rutiner? - Hvem har tilbud om produktet? - Konfigurering? - Anbefalinger?	
4.3	Anti-spyware/Adware - Rutiner? - Hvem har tilbud om produktet? - Konfigurering? - Anbefalinger?	
4.4	Vertsmaskinbasert Intrusion Detection System - Rutiner? - Hvem har tilbud om produktet? - Konfigurering? - Anbefalinger?	

4.5	Anti-Spam verktøy - Rutiner? - Hvem har tilbud om produktet? - Konfigurering? - Anbefalinger?	
4.6	Andre verktøy? - Bruksområder? - Erfaringer?	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

Sikkerhetsfremmende nettdesign

Omfang: Post 5 og 6.

Post nr	Sjekkpunkt	Merknader
5.0	**Struktur**	
5.1	Soneinndeling / Rollebasert adgang - Tanker om dette? - Har dere implementert noe slikt?	
5.2	Segmentering - Finnes det en form for segmentering av nettene i dag? - Hvis ja: - Hvordan er nettene segmentert? - Hvorfor er de segmentert slik? - Oppleves dagens segmentering som hensiktsmessig?	
5.3	Pakkefilter / Brannmur - Har alle nett pakkefilter? - Åpen / stengt ende på filter(et)? - Generelle sperre for «farlige» tjenester fra omverden? (NetBIOS, SMB...) - Egen sperre for utgående SMTP (port 25)? - Sperrer inn/ut/begge? - Unicast Reverse Path Forwarding?	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

5.4	Sikring av nettutstyr - Separat nett for administrasjon? - Hvordan er tilgangen organisert? - SNMP - TACACS - Konfigurasjonshåndtering? Backup? - SSH vs. Telnet	
5.5	Åpne tilgangspunkt i vrimleareal?	
5.6	Karantenenett - Finnes noe slikt? - Hvordan brukes eventuelt dette?	
5.7	Trådløse nettverk - Utbyggingsplaner og omfang? - Soneinndeling / Segmentering? - Kryptering? - 802.1X? - Planer for eduroam?	
5.8	Hjemmekontor - Restriksjoner på bruk? - Metode for aksess?	
5.9	VPN - Plassering av konsentrator? - Hvilke tjenester / nett er tilgjengelige vha. VPN? - Soneinndeling / Segmentering?	

5.10	Mobilitet - Hvordan håndteres mobile enheter som PDA og laptop? - Stilles det noen spesielle krav til slike enheter?	
5.11	Person-til-person kommunikasjon (VoIP/SIP) - Hvilke behov ser dere for slike tjenester? - Omfang? - Hvor? Eventuelt hvor ikke? - Dedikerte apparater? Eller «softphones» overalt?	
5.12	Oppringt / ISDN - Tilgang basert på brukernavn/passord (RADIUS)? - Tilbakeringing?	
5.13	IPv6 - Hvordan benyttes dette, og hvor? - Pakkefilter?	
5.14	Multicast - Lokalt Rendezvous-Punkt (For eksempel for å hindre uønsket annonsering av tjenester) ? - Bruksområder? - Hvem har tilgang?	
5.15	Autentisering og autorisasjon for nettilgang - Cisco NAC e.l.? - RADIUS? - TACACS(+)? - Andre?	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

Post nr	Sjekkpunkt	Merknader
6.0	**Tjenere**	
6.1	Web-tjener - Tiltenkt brukergruppe? - Eventuell plassering? - Separat intranett? - «Gamle kjenninger» som phpBB etc.?	
6.2	Fil-tjener - Tiltenkt brukergruppe? - Plassering? - Betjener denne flere nettsegmenter?	
6.3	Utskriftstjener - Tiltenkt brukergruppe? - Plassering? - Kvoter?	
6.4	Domenekontrollere og Active Directory - Separate domener for ulike brukergrupper? - Plassering av tjenere	
6.5	DHCP-tjener - Plassering? - Logging?	

6.6	DNS navnetjener - Plassering? - Separate publiserende og rekursive navnetjenere? - Finnes åpne, rekursive navnetjenere? - Er det etablert PTR-poster for alle tildelte adresseblokker?	
6.7	FTP-tjener - Tiltenkt brukergruppe? - Eventuell plassering? - Kontroll med bruken?	
6.8	IRC-tjener - Tiltenkt brukergruppe? - Eventuell plassering? - Kontroll med bruken?	
6.9	Andre tjenere - Plassering?	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

Lokal sikkerhetsovervåkning

Omfang: Post 7 og 8.

Post nr	Sjekkpunkt	Merknader
7.0	**Aktiv overvåkning**	
7.1	Verktøyportefølje - Nmap? - Nessus? - NAV? - Andre? - Savnes noen verktøy? (Også verktøy som ikke finnes)	
7.2	Plassering av sensorer	
7.3	Rapporter / Alarmer - Rutiner for kjøring?	
7.4	Erfaringer	

Institusjon: XX **Studiested: XX** **Bygg:** **Dato: xx.xx.xxxx**

Post nr	Sjekkpunkt	Merknader
8.0	**Passiv overvåkning**	
8.1	Portefølje - Netflow? - Stager? - NAV? - Intrusion Detection System? - Annet? - Savnes noen verktøy? (Også verktøy som ikke finnes)	
8.2	Monitorering - Logging/Sporing av private adresserom, f.eks. RFC1918-adresser, bak NAT e.l.?	
8.3	Rapporter / Alarmer	
8.4	Erfaringer	

– **Andre ting som er utelatt? Kommentarer?**