



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Egenevalueringsskjema

Endepunktsikkerhet

Dato: 24.11.2008
Versjon 1.0

Finanstilsynet
Tlf. 22 93 98 00
post@finansilsynet.no
www.finanstilsynet.no

Evalueringsskjema for foretakets sluttpunktsikkerhet

Rangering av prosess				Gjennom- ført dato:
-------------------------	--	--	--	------------------------

Antivirus – organisering

AV-OR1	Retningslinjer					
AV-OR2	Opplæring					
AV-OR3	Krav til leverandører av AV-løsninger					

Antivirus – funksjonalitet

AV-FU1	Krav til løsning					
AV-FU2	Installasjon					
AV-FU3	Konfigurasjon					
AV-FU4	Testing					

Antivirus - Lokal sikkerhet

AV-LS1	AV-løsning lokalt på PC og andre klienter					
AV-LS2	AV-løsning for hjemmekontor					

Antivirus - Server sikkerhet

AV-SS1	AV-løsning på servere					
--------	-----------------------	--	--	--	--	--

Antivirus – Overvåkning og Rapportering

AV-RA1	Overvåkning og Rapportering					
--------	-----------------------------	--	--	--	--	--

SPAM

SPAM1	Funksjonalitet					
SPAM2	Administrasjon og statistikk					

SPYware

SPY1	Installasjon					
SPY2	Test og overvåking					

	AV-OR1	Kontroll-spørsmål		Sårbarhet		
				H	M	L
Antivirus – organisering		Ja	Nei			
Retningslinjer						
1. Har virksomheten en oppdatert sikkerhetsstrategi?						
2. Har virksomheten oppdaterte og kjente retningslinjer for sikkerhet ?						
3. Er bekjempelse av ondsinnet kode, som for eksempel virus og trojanere, tatt inn som en del av virksomhetens retningslinjer for anti-virus løsninger?						
4 Er patch management for fortløpende håndtering av sårbarheter i operativsystem, tjenester eller applikasjoner som avdekkes, tatt inn som en del av virksomhetens sikkerhetspolicy/-strategi?						
5. Er det etablert retningslinjer som beskriver hvordan den enkelte bruker skal forholde seg til potensielle farer forbundet med ondsinnet kode?						
6. Er det etablert retningslinjer for etablering, drift og vedlikehold av AV-løsninger og patch management?						
7. Beskriver retningslinjene hvordan foretaket har sikret at det har tilgang til nødvendig kompetanse på området?						
8. Omfatter retningslinjene for drift av AV-løsningene rutiner for overvåking, dokumentasjon og rapportering av hendelser og status?						
9. Har virksomheten en sentral database over hardware og software som inneholder informasjon om elementenes lokasjon, konfigurasjon, vedlikehold og eierskap?						
10. Er det definert hvilke maskiner som skal ha AV-løsning installert?						
11. Dersom det er maskiner som ikke har AV-løsninger, er det krav i retningslinjene om at begrunnelsen for dette skal være dokumentert?						
12. Blir det utarbeidet detaljerte spesifikasjoner for innkjøp av IT-sikkerhetsløsninger, som for eksempel løsninger for anti-virus eller personlig brannmur?						
13. Utarbeides det detaljerte spesifikasjoner for innkjøp av løsninger for anti-virus, anti-spam og anti-spyware?						
14. Er det etablert avtaler som setter krav til driftsleverandørens AV-løsninger og patch management?						

	15. Beskriver avtalen med driftsleverandør dennes ansvar ved utbrudd av ondsinnet kode?			
	16. Foreligger det retningslinjer for håndtering av krisesituasjoner?			
	17. Er det etablert en plan for fjerning av ondsinnet kode?			
	18. Er det krav i retningslinjene til testing av plan for fjerning av ondsinnet kode?			
	19. Er retningslinjene gjenstand for jevnlig revisjon/oppdatering?			
	20. Justeres retningslinjene i henhold til anbefalinger fra leverandøren av AV-løsningene?			
<u>Kommentarer:</u>				

	AV-OR2	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Antivirus – opplæring					
	Opplæring	Ja	Nei			
	1. Er gjennomgang av retningslinjene for sikkerhet en del av opplæringen til nyansatte?					
	2. Er det klart definert hvilke konsekvenser brudd på retningslinjer og rutiner kan gi?					
	3. Er konsekvenser ved brudd på retningslinjer og rutiner formidlet til alle medarbeidere?					
	4. Har de ansatte fått opplæring i hvordan de skal rapportere mulige sikkerhetsbrudd?					
	5. Er det etablert retningslinjer for håndtering av Hoax ¹ ?					
	6. Får driftspersonell opplæring i drift av løsningene for anti-virus og anti-spam?					
	7. Gis det spesialopplæring i krisehåndtering for grupper som håndterer krisesituasjoner?					
	8. Gjennomføres det regelmessige holdningsskapende kampanjer?					
	9. Gjenspeiles bedriftens policy/retningslinjer/rutiner i det holdningsskapende arbeidet?					
<u>Kommentarer:</u>						

¹ Hoax er meldinger, som oftest e-post, til brukerne med et skremmende eller villedende innhold og kan forårsake skade hvis meldingen feilaktig blir oppfattet som troverdig og instruksjonene i den utført.

	AV-OR3	Kontroll- spørsmål		Sårbarhet		
				H	M	L
	Antivirus – organisering					
	Krav til leverandører av AV-løsninger	Ja	Nei			
	1. Har foretaket vurdert anti-virus løsningene til flere leverandører?					
	2. Foreligger det avtale om support med leverandøren?					
	3. Er det mulig å få teknisk støtte på stedet fra leverandøren?					
	4. Tilbyr leverandører opplæring på forskjellige nivåer?					
	5. Kan leverandøren tilby prioritert tilgang til support?					
	6. Er det etablert avtaler med eksterne spesialister for håndtering av krisesituasjoner?					
<u>Kommentarer:</u>						

	FU1 AV- Antivirus – funksjonalitet	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Krav til løsning	Ja	Nei			
	1. Benyttes det kun anerkjente løsninger for anti-virus og anti-spam?					
	2. Benyttes det AV-løsninger som kan finne både virus, trojanere, ormer og annen ondsinnet kode?					
	3. Benyttes det AV-løsninger som har evne til å finne modulære virus og polymorfisk ondsinnet kode?					
	4. Benyttes det AV-løsninger som har evne til å detektere adware ² og Hoax?					
	5. Er det spesifisert hvem som kan svare på og videresende Hoax?					
	6. Er det spesifisert hvor ofte det skal gjøres automatisk søk etter oppdateringer av AV-løsningen?					
	7. Kan det gjøres manuelle søk etter oppdateringer?					
	8. Er det spesifisert håndtering av virus det ikke finnes beskyttelse mot?					
	9. Er det kun autoriserte medarbeidere som behandler ondsinnet kode?					
	10. Er det etablert rutiner for automatisk søk etter og oppdatering med nye patcher for å tette hull når det avdekkes sårbarheter i operativsystem, tjenester eller applikasjoner?					
	11. Er det etablert rutiner for oppdatering med nye patcher av nettverksinfrastruktur (ruter, modem m.m.)?					
	12. Er det spesifisert hvor ofte det skal gjøres automatisk søk etter nye patcher?					
	13. Er det dokumentert hvilken programvare som skal ha automatisk patching?					

² anti-spyware er en bred kategori av software som har det til felles at programmene blir installert uten PC-brukerens viten og vilje og samler informasjon om PC-brukeren og hva denne foretar seg på nettet. En del anti-spyware er kjent som adware. Adware er selvinstallerende software som følger med nedlasting av gratis programvare. Adware kan blant annet medføre en overveldende mengde popups med reklame på brukers PC.

Kommentarer:

	AV-FU2	Kontroll- spørsmål		Sårbarhet		
				H	M	L
	Antivirus – funksjonalitet					
	Installasjon	Ja	Nei			
	1. Er det installert AV-løsninger på alle aktuelle maskiner tilknyttet virksomhetens nettverk?					
	2. Foreligger det en metode for å finne ut om alle aktuelle maskiner har AV-løsninger installert?					
	3. Foreligger det en metode for å finne ut om AV-løsning på en maskin har blitt slått av etter installasjon?					
	4. Er det verifisert at alle maskiner som skal ha AV-løsning installert, virkelig har det?					
	5. Kan installasjon, avinstallasjon, oppdateringer, konfigurasjon og rapportering foretas gjennom løsningsens eget administrasjonsverktøy eller gjennom kjente verktøy for dette formålet?					
	6. Kan AV-løsningene på alle maskiner tvinges til umiddelbar oppdatering fra sentralt punkt i nettverket?					
<u>Kommentarer:</u>						

	AV-FU3	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Antivirus – funksjonalitet					
	Konfigurasjon	Ja	Nei			
	1. Er AV-løsningene konfigurert i henhold til leverandørens spesifikasjoner?					
	2. Er AV-løsningene konfigurert av eksterne spesialister?					
	3. Søker AV-løsningene automatisk gjennom alle filer som åpnes?					
	4. Foreligger det en komplett oversikt over konfigurasjon, berørte systemkomponenter, versjoner og oppdateringer?					
	5. Kan filer, filtyper og områder spesifiseres for utelatelse fra gjennom søking?					
	6. Søker AV-løsningen regelmessig gjennom alle filer som ikke spesifikt er utelatt?					
	7. Har AV-løsningen ulike tilgangsnivåer for endring av konfigurasjon?					
	8. Er det etablert rutiner for manuell kontroll av virus i filer som sendes ut på andre medier enn over elektroniske linjer?					
	9. Er det lagt inn sperre for mottak av vedlegg som er av visse fil-typer (extention)?					
	10. Er det spesifisert hvilke rettigheter i AV-løsningen den enkelte bruker har?					
	11. Er konfigurasjonen av AV-løsningen dokumentert og dokumentasjonen versjonshåndtert?					
<u>Kommentarer:</u>						

	AV-FU4	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Antivirus – funksjonalitet					
	Testing	Ja	Nei			
	1. Foretas det test ved oppgradering av program i AV-løsningen?					
	2. Foretas det test i et begrenset miljø (pilot) ved oppgradering av program i AV-løsningen?					
	3. Foretas det test ved oppgradering av engine i AV-løsningen?					
	4. Benyttes EICAR teststreng når nye systemer skal innlemmes i AV-løsningen for å kontrollere at systemet fanges opp av AV-kontrollen?					
	5. Rapporteres problemer som avdekkes i testingen tilbake til leverandøren?					
<u>Kommentarer:</u>						

	AV-LS1	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Antivirus - Lokal sikkerhet					
	AV-løsning lokalt på PC og andre klienter	Ja	Nei			
	1. Kan AV-løsningen oppdateres uavhengig av virksomhetens nettverk, dersom maskinen benyttes separat fra nettverket?					
	2. Er AV-løsningene på lokale maskiner sikret mot at brukere som ikke er autorisert for det, kan endre hvilke filer og områder som skal skannes?					
	3. Er AV-løsningene på lokale maskiner sikret mot at de kan stoppes/avinstalleres av brukere som ikke er autorisert for det?					
	4. Dersom foretaket benytter IT-tjenester via mobile enheter som mobiltelefon eller PDA, er det etablert AV-løsninger på disse?					
<u>Kommentarer:</u>						

	AV-LS2	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Antivirus - Lokal sikkerhet					
	Krav til AV-løsning for hjemmekontor	Ja	Nei			
	1. Benyttes VPN for oppkopling til virksomhetens nettverk?					
	2. Stilles det krav om at hjemmekontormaskiner med tilgang til virksomhetens nettverk, har virksomhetsgodkjent AV-løsning installert?					
	3. Er det etablert retningslinjer som beskriver hvordan hjemmekontormaskiner konfigureres, alternativt at disse maskinene skal konfigureres av IT-drift avdelingen i virksomheten?					
	4. Er det inngått avtale om bruk av hjemmekontor med den enkelte medarbeider som beskriver partenes ansvar?					
	5. Kan medarbeiderne benytte privat PC i hjemmekontorløsningen?					
	6. Er det etablert rutiner for å sikre at PC'er som blir benyttet på utsiden av bedriften, blir oppdatert med siste versjoner av AV-løsninger og patcher?					
	7. Kan medarbeiderne tilknyttes virksomhetens nettverk uten at AV-løsningen kjører?					
<u>Kommentarer:</u>						

	AV-SS1	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Antivirus - Server sikkerhet					
	AV-løsning installert på servere	Ja	Nei			
	1. Er AV-løsning installert på virksomhetskritiske og andre relevante servere?					
	2. Hvis AV-løsning ikke er installert på alle servere, er årsaken til dette dokumentert for hvert enkelt server det ikke er installert på?					
	3. Er AV-løsning installert på gateway eller perimetermaskiner, for kontroll av trafikk inn og ut fra virksomhetens nettverk?					
	4. Er det sikret at enheter som ikke har godkjent AV-løsning installert, nektes adgang til tjenester i nettverket?					
	5. Er AV-løsningene konfigurert slik at brukere autoriseres for ulike tilgangsrettigheter?					
	6. Er det kun driftsansvarlig som kan endre listen over filer som utelates fra gjennom søking?					
	7. Er det kun driftsansvarlig som kan skru av all gjennom søking av filer?					
	8. Er det kun driftsansvarlig som kan skru av gjennom søking i sanntid?					
	9. Stilles det krav til tredjeparter som får tilgang inn i nettverket om gjennom søking av medbragt utstyr for ondsinnet kode før maskiner tilkobles?					
	10. Stilles det krav til tredjeparter som får tilgang inn i nettverket om oppdaterte AV-løsninger?					
	11. Er Network Admission Control (NAC)-løsning brukt for å autentisere brukere (inkl. tredjepart) av nettverket?					
<u>Kommentarer:</u>						

	AV-RA1	Kontroll-spørsmål		Sårbarhet		
	Antivirus – Overvåkning og Rapportering			H	M	L
	Overvåkning og Rapportering	Ja	Nei			
	1. Gjøres overvåkning av enheter tilkoblet nettverket i sann tid?					
	2. Er løsningen for overvåkning av tilkoblede enheter slik at den rapporterer enheter som ikke har godkjent AV-løsning installert?					
	3. Loggfører AV-løsningen funn av ondsinnet kode?					
	4. Rapporterer AV-løsningen funn av ondsinnet kode til spesifiserte maskiner / personer (SNMP, SMTP, GSM-SMS, Proprietære løsninger)?					
	5. Kan løsningen rapportere prioriterte utbrudd av ondsinnet kode?					
	6. Loggfører AV-løsningen alle oppdateringer?					
	7. Rapporterer AV-løsningen alle oppdateringer?					
	8. Kan rapporteringssystemet skille på type informasjon som skal rutes til ulike personer / grupper i virksomheten?					
	9. Kan rapporteringssystemet rapportere utløp av lisenser?					
	10. Kan rapporteringssystemet rapportere antall lisenser i bruk?					
	11. Kan rapporteringssystemet logge alle versjoner av program, engine og patterns i AV-løsningen?					
	12. Logger rapporteringssystemet alle patcher som legges på?					
	13. Bli rapportering som foregår over usikre linjer kryptert?					
	14. Bli rapporter og logger sikret ved lagring?					
	15. Verifiseres det at det ikke settes opp rapporteringsloop under implementering av løsningene?					
	16. Er det utpekt en ansvarlig for å kontrollere resultatet av rapporteringer fra AV-systemet og følge opp eventuelle avvik?					
	17. Bli resultatene fra rapportering og logger regelmessig gjennomgått?					

Kommentarer:

	SPAM1	Kontroll-spørsmål		Sårbarhet		
				H	M	L
Spam						
Funksjonalitet		Ja	Nei			
	1. Har anti-spam-løsningen personlige postbokser dedikert til e-post som mistenkes å være spam?					
	2. Kontrollerer hver medarbeider jevnlig postboks for mistenkelig e-post, for om e-postene er spam?					
	3. Inneholder anti-spam-løsningen en sentral Black-list?					
	4. Får anti-spam-løsningen oppdatert lister over kjente ord og uttrykk som er typiske for spam både i tittelfeltet og i hovedtekst feltet?					
	5. Sjekker anti-spam-løsningen avsenders e-postadresse, for om den inneholder uforholdsmessig mange sifre?					
	6. Sjekker anti-spam-løsningen antall mottakere av e-posten?					
	7. Kontrollerer anti-spam-løsningen Mime header, for om SMTP-from og Mime-from er like?					
	8. Kontrollerer anti-spam-løsningen Mime header, for om Mime-from er tom?					
	9. Kontrollerer anti-spam-løsningen Mime header for om Mime-from feltet er korrekt?					
	10. Kontrollerer anti-spam-løsningen om det benyttes remote images?					
	11. Sjekker anti-spam-løsningen begynnelsen av e-posten for om den starter med bruker-id?					
	12. Kontrollerer anti-spam-løsningen om det er uvanlig tegnbruk i tittelfeltet?					
	13. Benytter anti-spam-løsningen DNS lookup?					
<u>Kommentarer:</u>						

	SPAM2	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Spam					
	Administrasjon og statistikk	Ja	Nei			
	1. Kan anti-spam løsningen driftes over nettverk?					
	2. Kan anti-spam løsningen levere rapporter og statistikk over mottatt spam?					
	3. Kan anti-spam løsningen levere rapporter for hvilken teknologi som reagerer på og definerer e-post som spam?					
	4. Kan det tas ut statistikk som viser hvilke adresser som mottar ulike mengder spam?					
	5. Kan det tas ut statistikk som viser hvor mye spam det kommer i ulike tidsrom eller perioder?					
<u>Kommentarer:</u>						

	SPY1	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Spion-programmer					
	Installasjon	Ja	Nei			
	1. Er det installert løsninger for deteksjon og fjerning av spyware på alle maskiner tilknyttet virksomhetens nettverk?					
	2. Er det installert løsninger for deteksjon og fjerning av adware?					
	3. Kan installasjon, avinstallasjon, oppdateringer, konfigurasjon og rapportering foretas gjennom løsningens eget administrasjonsverktøy eller gjennom kjente verktøy for dette formålet?					
	4. Er det verifisert at alle maskiner som skal ha spy-ware beskyttelse installert, virkelig har det?					
	5. Foreligger det metoder for å finne ut om alle aktuelle maskiner har anti-spyware beskyttelse installert?					
<u>Kommentarer:</u>						

	SPY2	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Spion-programmer					
	Test og overvåkning	Ja	Nei			
	1. Foretas det jevnligte tester for kontroll av at løsningen fungerer?					
	2. Foretas det akseptansetest før utrulling i virksomhetens nettverk, for å verifisere at løsningen fungerer godt sammen eksisterende program- og maskinvare?					
	3. Blir all anti-spyware beskyttelse testet før innkjøp?					
	4. Er det installert tekniske løsninger som overvåker at anti-spyware beskyttelse er installert og aktiv på alle enheter koblet til nettverket?					
	5. Er det utpekt en ansvarlig for å kontrollere logger fra overvåkingen og følge opp eventuelle avvik?					
	6. Har anti-spyware beskyttelsen evne til å detektere potensielle sikkerhetsrisikoer?					
	7. Er det kun autoriserte medarbeidere som behandler anti-spyware?					
<u>Kommentarer:</u>						