



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Egenevalueringsskjema

Brannmur

Dato: 24.11.2008

Versjon 1.0

Finanstilsynet

Tlf. 22 93 98 00

post@finansilsynet.no

www.finanstilsynet.no

Evalueringsskjema for foretakets brannmur

Rangerin g av prosess					Gjennom- ført dato:
-----------------------------	--	--	--	--	------------------------

Brannmur 1	Organisering/styring/kontroll					
Brannmur 2	Kartlegging og analyse					
Brannmur 3	Etablering og implementering					
Brannmur 4	Endringshåndtering					
Brannmur 5	Stateful inspection/ dynamic packet filtering (SI/DPF)					
Brannmur 6	Pakkefiltrering					
Brannmur 7	Proxy brannmur					
Brannmur 8	DMZ					
Brannmur 9	Konfigurering					
Brannmur 10	Overvåking, revisjon og reaksjon på hendelser					
Brannmur 11	Backup and recovery					

	Brannmur 1	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Organisering/styring/kontroll	Ja	Nei			
	1. Omhandler sikkerhetspolicyen temaet brannmur?					
	2. Foreligger det en egen policy for foretakets bruk av brannmur?					
	3. Ved gjennomføring av ROS analyse, foreligger det retningslinjer for hvordan en målrettet og fullstendig analyse rettet mot de områder en brannmur kan sikre skal skje?					
	4. Er det rutiner som sikrer at alle parter som har ansvar for foretakets tjeneste på nettet kommuniserer hvilke sikkerhetselementer som leveransen inkluderer? (Sikkerhet kan være implementert i alle lag, fra applikasjonslaget til nettverkslaget. Det er avgjørende at utviklings-, drifts- og nettverksansvarlig samt administrator vet hvilke sikring som er implementert i de ulike lagene. Bare da kan en total sikring oppnås. Det er ledelsen ansvar å påse at denne koordineringen sikres).					
	5. Blir kravene til sikkerhet tatt inn som en del av kravspesifikasjonen som danner grunnlag for systemutviklingen/anskaffelse for applikasjoner som skal være tilgjengelige på Internet og de applikasjoner som installeres på brannmuren?					
	6. Blir det verifisert at loggingen i brannmuren fungerer som forutsatt?					
	7. Foreligger det en rutine for vedlikehold av brannmurregler?					
	8. Er SW oppdatert til siste nivå?					

	9. Er det etablert rutiner som sikrer gjennomgang av system og applikasjonslogger for å avdekke angrep?			
	10. Er det etablert rutiner som sikrer at sikkerhetsrelaterte hendelser formidles til systemansvarlig?			
	11. Er det etablert rutiner for konfigurasjonshåndtering for HW og SW på brannmuren?			

Kommentarer:

	Brannmur 2	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Kartlegging og analyse	Ja	Nei			
	1. Er det gjennomført analyser for å kartlegge og vurdere eksisterende nettverk, identifikasjon av alle oppkoblinger, hvilken type trafikk som er autorisert, brannmurreglene og alarm og varslingsrutiner?					
	2. Basert på analysen i 1, har foretaket analysert og vurdert hvilken type brannmurkonfigurasjon som er best egnet for foretaket, eksempelvis pakkefiltrering, stateful inspection, proxy server?					
	3. Inngår vurderinger knyttet til Single Point of Failure i vurderingen i pkt. 2? (Eks. Hvis all trafikk går gjennom et en "trang" DMZ, for eksempel gjennom en (1) proxy server, så blir virksomheten sårbar dersom proxy server er utilgjengelig).					
	4. Har foretaket vurdert om de har tilstrekkelig kompetanse internt for å ivareta brannmursikringen?					
	5. Har foretaket vurdert å benytte følgende tiltak i tillegg til brannmur? <ul style="list-style-type: none"> • Nettverks basert IDS • Personal firewall/intrusion prevension for å beskytte WS og servere mot ondartet trafikk over lovlige porter i FW • Antivirus programvare • E-mail and Web innholdsfiltrering • URL filtrering • Tredjeparts autentiseringsprogramvare 					
	6. Kjøres det antivirus på klientene?					

	7. Brannmur hindrer ikke angrep som stammer fra innsiden av nettverket. Er det implementert rutiner som sikrer mot slike, som for eksempel brukerpolicy, personlig brannmur/intrusion prevention, nettverksovervåking, filtrering og tilgangskontroll på alle maskiner, segmentering av nettverk i sone som krever høy sikring vs. sone som krever mindre høy sikring?			
--	--	--	--	--

Kommentarer:

	Brannmur 3	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Etablering og implementering	Ja	Nei			
	1. Er det prosedyrer som benyttes for å analysere applikasjoner før de går i produksjon for å avdekke svakheter i disse (se for eksempel Finanstilsynets modul "Web Programmering" der en rekke mulige svakheter og mottiltak er listet)?					
	2. Er det etablert rutiner som sikrer arbeidsdeling når det gjelder utvikling testing og produksjonssetting av programmer som går på Internet?					
	3. Er det etablert autorisasjonsrutiner/kontroller når det gjelder pålogging fra eksterne?					
	4. Er det etablert rutiner og prosedyrer når det gjelder (tildeling av) tilgang til funksjoner for administrasjon av brannmuren for å sikre at ikke uvedkommende kan få tilgang til denne, verken logisk eller fysisk?					
	5. Tilsvarende som 7, for fjerntilgang?					
	6. Er det etablert prosedyrene for overvåking av logger for å sikre rask og effektiv håndtering av uønsket trafikk?					
	7. Er det etablert prosedyrer for håndtering av potensielle og reelle angrep?					
	8. Er det etablert en rutine for risikoanalyse? Følges denne?					
	9. Dersom det er mulig å kople seg opp til virksomhetene over Internet ved hjelp av VPN, følger VPN oppsettet best practice? (Engangspassord, session time out osv.).					

	10. Er det etablert rutiner og prosesser for gjennomføring av penetrasjonstesting, herunder kriterier for når ny testing skal gjennomføres etter endringer? Hvordan følges funn i penetrasjonstestene opp?			
	11. Er brannmur og nettverksutstyr som knytter den til nettverksinfrastrukturen fysisk beskyttet i tilstrekkelig grad?			
	12. Kjører brannmuren på et herdet og oppdatert operativsystem? Foreligger det en konfigurasjonsprosess som benyttes i håndteringen av brannmur?			
	13. Finnes det en person som er ansvarlig for å følge kontinuerlig med på brannmurleverandørens sikkerhets publikasjoner og som implementerer anbefalte og relevante tiltak?			
<u>Kommentarer:</u>				

	Brannmur 4	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Endringshåndtering	Ja	Nei			
	<p>1. Er det etablert prosedyrer for vedlikehold av regelverket i brannmuren, som for eksempel gjennomgang av tilganger til vedlikeholdsfunksjoner, rutiner for å lage endringsforespørsel, nye eller endrede testprosedyrer, produksjonssetting og dokumentasjon? Inneholder vedlikeholdsrutinen krav til forespørsel, endring, test, produksjon og dokumentasjon, for eksempel slik at</p> <ul style="list-style-type: none"> a. endringsforespørslene skal inneholde behov og eierskap, dato for implementering og eventuelt hvor lenge denne regelen skal fungere. b. løsningene skal være gjennomgått av kvalifisert personell som forstår risikoaspektet ved endringen. Risikoen skal dokumenteres i forhold til den helhetlige IT infrastrukturen. c. alle interfacer i alle retninger er testet, med og uten brannmurregler på, for å teste hvor sårbar du er når brannmuren ikke virker skikkelig. (Den minste endring i brannmuren systemet eller regelsett kan totalt endre sikkerheten i brannmuren). d. godkjennelsesprosessen inkluderer godkjenning av leder av brannmur administrasjonen og eier av forretningsområdet. e. brannmuren og reglene gjennomgår formelle tester i et testmiljø før den legges inn i produksjonsmiljøet. 					

	Brannmur 4	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Endringshåndtering	Ja	Nei			
	<ul style="list-style-type: none"> f. sårbarhetstester av brannmuren gjennomføres regelmessig med tanke på hvor robust den er mot de mange nye exploits som dukker opp. g. prosedyrer for godkjenning av resultatene av sårbarhetstesting av brannmuren. h. prosedyrer for å teste nytt SW og hvordan dette konfigureres for å oppfylle satte krav. 					
<u>Kommentarer:</u>						

	Brannmur 5	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Stateful inspection/ dynamic packet filtering (SI/DPF)	Ja	Nei			
	1. Bekreft at alle kontroller er implementert i alle API dersom API i SI/DPF benyttes.					
	2. Er det gjennomført tester som viser at trafikk som påvirkes av SI/DPF fungerer tilfredsstillende? (SI/DPF bruker state tables og programmerte instruksjoner. Det brukes informasjon fra packet header og fra innholdet i pakken opp gjennom applikasjonslaget. Informasjoner blir prosessert og lagret for å tilrettelegge for at brannmuren kan klassifisere innholdet i trafikken og spore all trafikk knyttet til en oppkobling (sesjon). Prinsippet er å identifisere pakker som er del av en oppkobling og åpne og stenge spesifikke porter for den trafikken).					
	3. Eksempler på hva som bør sees på når en går igjennom filtrering er gateways, FTP, X Windows, DNS og faste adresser. Er det kontrollert at brannmuren: <ul style="list-style-type: none"> • bare tillater adgang til de adresser det er meningen skal ha tilgang utenfra • hindrer uautorisert bruk av services som FTP og Telnet • hindrer bruk av spesielle porter • kun tillater pakker som kommer fra autoriserte sites fra eksterne nettverk. All annen trafikk slettes. 					
	4. Er det rutiner som sikrer regelmessig gjennomgang av regler for tilgangskontroll eller andre tiltak som er iverksatt for å håndtere uønskede angrep som DDOS angrep mot devices?					
	5. Er det iverksatt tiltak som hindrer IP spoofing?					

	6. NAT bør benyttes - benyttes NAT i virksomheten?			
	7. Er inngående trafikk tillatt bare når en godkjent oppkopling er satt opp fra innsiden?			
	8. Dokumenter hvordan en SI/DPF vil påvirke de kontroller som andre brannmurer har når SI/DPF er benyttet som kantbrannmur og det er andre brannmurer bak denne.			

Kommentarer:

	Brannmur 6	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Pakkefiltrering	Ja	Nei			
	<p>1. Er pakkefiltreringen satt opp slik at:</p> <ul style="list-style-type: none"> • tilgang begrenses til de adresser som skal kunne nås fra utsiden • det ikke er lov til å bruke uautoriserte tjenester som ftp og telnet • det ikke er tilgang til nærmere definerte porter • den tillater pakker som kommer fra autoriserte siter fra eksterne nettverk (hvis relevant) • sletter all source-routed traffic 					
	2. Er det implementert regler for å kunne droppe uønsket kommunikasjon som for eksempel DDOS?					
	3. Er det etablert regler for å hindre IP spoofing?					
	4. Sikrer foretaket seg at de filtrerer pakker for korrekt adresse basert på SANS topp 20 sårbarheter http://www.sans.org/top20/ ?					
	5. Sikrer foretaket seg at de filtrerer og slår av alle unødvendige porter og sårbare porter basert på SANS topp 20 sårbarheter http://www.sans.org/top20/ ?					
	6. NAT bør benyttes - benyttes NAT i virksomheten?					
	7. Er inngående trafikk tillatt bare når en godkjent oppkopling er satt opp fra innsiden?					

	<p>8. Har foretaket vurdert følgende svakheter ved pakkefiltrering:</p> <p>Det er lite eller ingen loggings kapasitet hvilket medfører at administrator vanskelig kan se om en ruter er kompromittert eller er under angrep</p> <p>Pakkefiltrering er ofte vanskelig å teste slik at en åpner for utestede svakheter.</p> <p>Dersom komplekse filterregler er etablert kan dette medføre at regelverket blir vanskelig å administrere.</p> <p>Hver enkelt datamaskin som er direkte tilgjengelig fra Internett, vil trenge en egen kopi av de avanserte autentiseringstiltakene.</p>			
<p><u>Kommentarer:</u></p>				

	Brannmur 8	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	DMZ	Ja	Nei			
	1. Er systemene i DMZ segmenter synlige for eksterne brukere?					
	2. Dersom eksterne tjenesteleverandører kan utføre problemløsning på utstyr som ligger i DMZ segmentet hvor oppkobling med tjenesteleverandøren gjøres, har foretaket utført tester som presist kartlegger omfanget av DMZ nettverket og hvilke risiko tjenesteleverandørs tilganger representerer?					
	3. Har foretaket gått gjennom DMZ nettverket og testet dette for å sikre at eksterne ikke kan administrere eller konfigurere <ul style="list-style-type: none"> • brannmuren • nettverkskomponenter og systemer i DMZ segmentet? 					
	4. Har foretaket verifisert at aksess kontroll regler er implementert på alle nettverkskomponenter som er tilknyttet den ytterste brannmuren?					
	5. Har foretaket gjennomgått reglene for brannmur og bekreftet at alle pakker ved default forkastes unntatt når pakkene gis lovlig adgang i følge de oppsatte reglene men da bare til systemer som ligger i DMZ segmentet?					
	6. Har foretaket gjennomgått, testet og bekreftet at alle systemer i DMZ segmentet er satt opp slik at disse ikke kan kommunisere uten gjennom brannmuren?					
	7. Dersom systemer i DMZ kan kommuniserer utenom brannmuren, har foretaket vurdert risikoen ved dette?					

	<p>8. Er systemer i DMZ segmentet satt slik opp at de ikke kan initiere kommunikasjon med system og komponenter på innsiden? Dersom ikke dette er tilfellet, er risikoen ved dette vurdert?</p>			
	<p>9. Har foretaket kontrollert at nettverkskomponenter, brannmurer og system i DMZ nettverket er satt opp slik at</p> <ul style="list-style-type: none"> • all kommunikasjon mellom alle mulige kombinasjoner av komponenter, brannmurer og systemer er definert • all trafikk gjennom og ut fra DMZ nettverket er lett identifiserbart • rutingen er satt så stramt at bare autorisert trafikk går igjennom? 			
	<p>10. Har foretaket testet at NAT fungerer i henhold til sikkerhets policy og at konfigurasjonen verifiseres jevnlig av godkjent personal?</p>			
	<p>11. Er brannmuren satt opp</p> <ul style="list-style-type: none"> • til å hindre alle pakker som kommer utenfra som har source IP adresser brukt i det interne nettverket • til å hindre alle pakker som kommer innenfra som har source IP adresser som ikke er interne adresser? 			
	<p>12. Er brannmuren satt opp slik at den varsler når brannmuren scannes på de mest vanlige portene, selv om det ikke er systemer som bruker disse?</p>			
	<p>13. Er brannmuren satt slik opp at den ikke gir melding tilbake når en pakke er forkastet?</p>			
	<p>14. Er brannmuren testet ved å scanne alle segmenter inkludert DMZ for å sikre at pakker ikke kan komme gjennom? (Dokumenter at resultat er i samsvar med sikkerhets policy).</p>			

	<p>15. Er alle reglene i brannmuren er i henhold til sikkerhets policy?</p> <p>(Dette gjøres ved å få tilstrekkelig informasjon om konsistens er tilstede ved å gå gjennom følgende komponenter av potensielle lovlige pakker; protokoll, avsender IP adresse, mottager IP adresse, avsender port og mottager port. Kombinasjoner av målsystem og port i en regel skal gi mening for målsystemet i DMZ segmentet. En regel skal være tilpasset systemets funksjoner i DMZ segmentet, og skal tillate systemer på det interne nettverket å initiere kommunikasjon med systemer i DMZ segmentet og tillate systemer i DMZ segmentet å svare på kommunikasjon initiert fra innsiden. Hvis det er for mange regler som skal testes, kan dette indikere dårlig sikkerhetsarkitektur som gjør brannmuren vanskelig å administrere).</p>			
	<p>16. Er det regler i brannmuren som stopper all trafikk over TCP og UDP på porter over 1023?</p>			
	<p>17. Dersom det ikke er regler i brannmuren som stopper all trafikk over TCP og UDP på porter over 1023, er risikoen vurdert og er det iverksatt kompenserende tiltak?</p>			
	<p>18. Dersom det er etablert flere fysiske brannmurer i DMZ nettverket for failover, tilgjengelighet eller speiling, er det da etablert tiltak som sikrer at alle brannmurene har samme konfigurasjon?</p>			
<p><u>Kommentarer:</u></p>				

	Brannmur 9	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Konfigurering	Ja	Nei			
	1. Er brannmuren konfigurert til å "deny all services, unless explicitly allowed"?					
	2. Er antallet applikasjoner som går på brannmuren begrenset slik at brannmuren kan gjøre det den er best til?					
	3. Er det vurdert å kjøre antivirus, innholdsfiltrering, VPN, DHCP og autentiserings software på dedikerte systemer bak brannmuren? (DNS, e-post load balancing service eller annen programvare som ikke er relatert til brannmurspesifikk funksjoner skal ikke være installert eller prosessert av brannmuren).					
	4. Er brannmuren satt slik opp at den begrenser SNMP (System Network Management Protocol) spørringer?					
	5. Er brannmuren satt slik opp at den blokkerer for ikke lovlige porter, selv om det foran brannmuren står en ruter som gjør det samme? (Tilgangslistene i ruter er ikke tilstrekkelig for å oppfylle sikkerhetsnivået for en brannmurløsning. En ruter er bare en del av en brannmurløsning. Ruterene har typisk den funksjon at den avlaster brannmuren ved at ruterene bare slipper godkjente porter gjennom til brannmuren, istedenfor at brannmuren må filtrere alle innkomne porter. For alle tilfellers skyld skal det i brannmuren likevel blokkeres for porter som ikke er i bruk).					
	6. Er brannmuren satt slik opp at den ikke viser intern nettverksinformasjon til eksterne?					

	7. Er NAT benyttet for alle interne nettverksnoder som har lov til å kommunisere med eksterne nettverk?			
	8. UDP baserte tjenester bør ikke benyttes dersom det kan unngås. Har foretaket vurdert dette?			
	9. Har foretaket implementert skanning, filtrering eller blokking av Java, JavaScript og Activex?			
	10. Er det regler som begrenser bruken av NNTP tjenester til brukere som trenger denne tjenesten?			
	11. Benyttes statisk ruting i stedet for rutingprotokoller i de tilfeller der dette er mulig?			
	12. Er det implementert streng sikkerhetspolicy for de komponenter hvor brannmur er installert?			
	13. Er det etablert prosedyrer for å verifisere at sikkerhetspolicy etterleves?			
	14. Er det innført begrenset tilgang til brannmurgenererte logger for å forhindre uautoriserte slettinger og endringer?			
	15. Er alle sikkerhetsoppdateringer for alle komponenter i brannmur løsningen installert?			
	16. Kjører brannmurtjenestene under en unik bruker istedenfor som administrator eller root?			
	17. Er default administrator eller root passord endret? (Passordet skal ikke finnes i noen dictionary, skal være minst 8 karakterer langt og skal være en kombinasjon av store og små bokstaver, tall og andre karakterer som \$, % og @, og det skal byttes ofte).			

Kommentarer:

	Brannmur 10	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Overvåking, revisjon og reaksjon på hendelser	Ja	Nei			
	1. Eksisterer det rutiner for D/R og eksistere det kontinuitetsplaner for brannmuren?					
	2. Tas regelmessig sikkerhetskopi av brannmur konfigurasjonsfiler?					
	3. Lagres sikkerhetskopiene offsite?					
	4. Kontrolleres det regelmessig, minst hvert år, at brannmuren er satt opp som forutsatt i sikkerhetspolicy?					
	5. Er alle regler som er satt i sikkerhetspolicy og retningslinjer implementert?					
	6. Inneholder rutinene regler for hvordan svakheter som avdekkes i penetrasjonstesten skal følges opp?					
	7. Er det etablert rutiner for kontinuerlig overvåking av brannmur?					
	8. Blir all aktivitet på brannmuren logget?					
	9. Er det etablert overvåking av sensitive filer på brannmuren?					
	10. Blir loggene regelmessig gjennomgått?					
	11. Blir informasjonen i loggene behandlet som forretningsinformasjon og inkludert i data lagrings policy?					
	12. Blir det tatt regelmessig sikkerhetskopi av brannmurlogger (helst write-once)? Blir disse lagret for mulig fremhenting?					
	13. Benyttes en sikker remote syslog server for backup? (Dette gjør det vanskelig å modifisere/manipulere loggen).					

	14. Er det etablert egne tiltak, f. eks. IDS, på særlig høyrisiko tilkoblinger?			
--	---	--	--	--

Kommentarer:

