

TUNIX Beveiligingsbeleid

(Final)



**TUNIX keeps your
security up !**

Eigenaar: Leo Willems
Afdeling: Directie
Project: TUN/TUN=Directie

Dit document is het laatst geauditeerd door Ronald Pikkert op 02-02-2008.
De informatie in dit document is geldig tot 01-01-2010.

Versie: 1.10
Formatted: 14-11-2008
Copyright 2008 TUNIX Internet Security & Opleidingen



1. TUNIX Beveiligingsbeleid

1.1 Inleiding

Dit document is opgesteld ten behoeve van bestaande en potentiële TUNIX-klanten voor managed services en hosting-services. TUNIX realiseert zich dat beveiliging en het daarmee samenhangende bewustzijn niet een enkel product of een enkele dienst is, maar een voortdurend proces en een denkwijze. Dit document schetst een beeld van de beveiligingsprocessen bij TUNIX.

Het document biedt:

- een inleiding over TUNIX en zijn Security Organization;
- een overzicht van het beveiligingsbeleid en -programma van TUNIX, met nadruk op de sleutelementen en -initiatieven voor de beveiliging van gegevensnetwerken ter bescherming van TUNIX-klanten en hun gegevens terwijl deze door TUNIX worden beheerd of aanwezig zijn op het TUNIX-netwerk;
- een samenvatting van de beveiligingsverantwoordelijkheden van de klant ter bescherming van zichzelf.

Bezoek voor meer informatie over TUNIX onze website: <http://www.tunix.nl> of neem contact op met uw TUNIX account manager.



2. Disclaimer

Dit document geeft slechts een beperkt overzicht van het beveiligingsbeleid en -programma van TUNIX. Alleen al de aard van het op een hoog niveau houden van een beveiligingsinstelling maakt dat TUNIX in een publiek document geen details kan prijsgeven met betrekking tot het beveiligingsbeheer en de daarbij toegepaste hulpmiddelen/processen.

Dit document wordt alleen ter informatie verstrekt. Het is geen contractueel document en kan door geen enkele rechtspersoon worden uitgelegd als aanleiding gevende tot enige vertegenwoordiging of garantie van welke aard dan ook of enige verbintenis, verplichting of verantwoordelijkheid van de kant van TUNIX of enige andere rechtspersoon. De contractuele verplichtingen tussen TUNIX en zijn klant worden exclusief uiteengezet in een geschreven contract met de klant dat door beide partijen wordt ondertekend, en niets in dit document voegt iets toe aan, verwijdert iets uit, wijzigt iets aan of heeft anderszins invloed op een dergelijke overeenkomst. TUNIX behoudt zich het recht voor het beleid en de procedures die in dit document worden beschreven zonder kennisgeving aan of overleg met enige klant of andere rechtspersoon te wijzigen. Elk vertrouwen dat de lezer stelt in de inhoud hiervan komt geheel voor risico van de lezer; TUNIX biedt geen enkele representatie of garantie, expliciet noch impliciet, met betrekking tot de resultaten van het toepassen van de in dit document geschetste beveiligingsprocedures. Bovendien zijn TUNIX-klanten zelf verantwoordelijk voor het handhaven van beveiligingsbeleid en -programma's die op hun onderneming zijn afgestemd.



3. TUNIX Security Organization

TUNIX neemt deel in of monitort diverse wereldwijde beveiligingsorganisaties zoals

- CERT/CC
- Cert/NL (govcert.nl)
- Beveiligingsactiviteiten binnen de Internet Engineering Task Force (IETF)
- SANS
- The World Wide Web Consortium (W3C)
- Forum of International Response and Security Teams (FIRST) Team.

Mandaat van de Security Organization

TUNIX beschouwt netwerkbeveiliging als een hoeksteen van de wereldwijde diensten die zij levert. Door het beveiligingsbeleidsmandaat van het management van TUNIX verplicht TUNIX zichzelf haar klanten en zijn eigen informatie en bronnen te beschermen tegen ongeoorloofde toegang, openbaring, corrumpering of ontwrichting van diensten. Dit beveiligingsbeleid is van toepassing op netwerkelementen, systemen, toepassingen en werkstations in het bezit van of beheerd door TUNIX.

De uitvoer van het beleid wordt geleid door de TUNIX Security Organization die als taken heeft:

- de beveiligingsnormen en -richtlijnen van TUNIX in bezit te hebben en te beheren, en de uiteindelijke verantwoordelijkheid te dragen voor alle aspecten van netwerkbeveiliging binnen de onderneming;
- de bij TUNIX in bezit zijnde en door TUNIX beheerde bezittingen te beschermen;
- de beveiliging te leiden en de onderneming strategisch richting te geven;
- op een consistente manier de naleving van het netwerkbeveiligingsprogramma te garanderen;
- te garanderen dat de beveiligingsnormen van TUNIX worden geïmplementeerd en toegepast;



- de verantwoordelijkheid van leidinggevenden voor naleving van de beveiliging te garanderen;
- een beveiligingsherzieningsprogramma voor het vaststellen van de mate van naleving te coördineren;
- het bewustzijn over veranderingen en trends in de beveiligingsindustrie te onderhouden;
- het beveiligingseducatieprogramma binnen de onderneming te ontwikkelen en te beheren;
- beveiligingswaarschuwingen en advies te geven aan de serviceorganisatie;
- indien vereist specialistische beveiligingsondersteuning te bieden aan operationele en beveiligingsteams;
- de naleving van wet- en regelgeving t.a.v. beveiliging te monitoren en te ondersteunen.

Naleving van de beveiliging is een centraal punt in onze cultuur en is een voorwaarde voor de arbeidsrelatie. Elke management- en stafmedewerker is zich bewust van zijn of haar verantwoordelijkheid en dient de regels voortdurend na te leven.

De volgende paragraaf schetst enkele van de beveiligingsverantwoordelijkheden van elke TUNIX-medewerker:

Het management:

- is verantwoordingsplichtig voor het beschermen van goederen die het bezit of beheert;
- is verantwoordelijk voor het intrekken van logische en fysieke toegangsrechten van een medewerker bij zijn/haar hernieuwde taaktoewijzing of beëindiging van de arbeidsrelatie;
- is verantwoordelijk voor het door zijn medewerkers naleven van de vereisten van de TUNIX-beveiligingsnormen;
- is verantwoordelijk voor het met regelmatige tussenpozen uitvoeren van hervalidatie van de logische en fysieke toegang;
- is verantwoordelijk voor het ontwikkelen van vaardigheden bij de medewerkers, die nodig zijn om de beveiligingsfuncties te ondersteunen;
- is verantwoordelijk voor het regelmatig met de medewerkers herzien en aanvaarden van de Acceptable Use Policy (gedragscode).

De medewerkers:



- dienen de TUNIX-beveiligingsnormen na te leven;
- dienen de processen ter controle van de beveiligingsstatus, upgrades van beveiligingsprofielen/-kenmerken, etc. op systemen onder hun beheer te handhaven en uit te voeren;
- dienen hun persoonlijke logische en fysieke toegangen tot systemen en faciliteiten regelmatig te valideren;
- dienen de eisen m.b.t. vertrouwelijkheid en de *clean desk*-kantoorprogrammas voor het beschermen van vertrouwelijke informatie na te leven;
- dienen de Acceptable Use Policy (gedragscode) na te leven.



4. Beveiligingsprogramma

Ook het beste ontwerp en de beste implementatie van netwerkbeveiliging dienen voortdurend te worden beheerd. TUNIX ziet netwerkbeveiliging als een proces dat wordt aangedreven door het bewustzijn bij management en gebruikers en wordt ondersteund door specialistische vaardigheden en geavanceerde technologie. Het beveiligingsprogramma implementeert het beveiligingsbeleid door middel van een verzameling aan initiatieven, processen en procedures die worden beheerd door de TUNIX Security Organization. Doel van het programma is informatie en bronnen van zowel TUNIX als alle klanten te beschermen. Ons beveiligingsprogramma concentreert zich op de volgende interne processen:

Controlemaatregelen voor fysieke toegang

TUNIX opereert in een beveiligde omgeving waarin fysieke toegang tot servicebeheercentra wordt gemonitord en beheerd. TUNIX past vele strategieën toe om deze bezittingen, en in het bijzonder het netwerk van TUNIX, te beveiligen, namelijk door:

- de toegang tot en bewegingen binnen de faciliteiten van TUNIX te beperken en te monitoren door middel van fysieke monitoring;
- de toegang te screenen met behulp van veiligheidspersoneel en/of technische middelen zoals geautomatiseerde toegangssystemen met kaarten;
- periodiek onderzoeken en audits naar fysieke beveiliging van zijn faciliteiten/locaties uit te voeren.

Controlemaatregelen voor logische toegang

De controle op logische toegang is gebaseerd op het principe van *least privilege*. Een gebruiker die toegang wil verkrijgen tot beveiligingssystemen van TUNIX of een klant moet daarvoor een actuele zakelijke noodzaak hebben, moet een unieke identificatie hebben gekregen (een speciaal operator-ID, niet de normale gebruikers-ID), en moet bekrachtigen dat hij/zij is wie hij/zij zegt te zijn. De volgende controleprocessen worden toegepast om de logische toegang te beheren:



- Authenticisering is het proces van het aantonen van een geclaimde identiteit tot tevredenheid van een toegangsrechten verlenende autoriteit.
- Elke individuele gebruiker moet positief en uniek zijn geïdentificeerd voordat toegang wordt verleend. Authenticisering van de gebruiker wordt bereikt met behulp van diverse methoden zoals: wachtwoorden, PINs (persoonlijke identificatienummers) en tokens.
- Het principe van *least privilege* garandeert dat elke toegang tot computerbronnen wordt beperkt tot alleen die opdrachten, gegevens en systemen die nodig zijn om de geautoriseerde functies uit te voeren.
- De administratie van toegangscontrolemaatregelen beperkt de toegang tot gevoelige informatie door geautoriseerde medewerkers en systeemnetwerkprocessors en beperkt de mogelijkheden om beveiligingsfuncties van het systeem in te stellen, te wijzigen of uit te schakelen. De geprivilegieerde toegang tot systeem- en netwerkelementen wordt streng gecontroleerd.
- Het loggen van audits resulteert in een record voor elke succesvolle en mislukte toegangspoging. Verdachte toegangspogingen worden als schendingen van de beveiliging herkend en gerapporteerd.

Toegangsvalidatieproces

Alleen TUNIX-medewerkers met een actuele zakelijke noodzaak krijgen een autorisatie voor fysieke en logische toegang tot security-faciliteiten en -systemen.

Alle managers zijn verplicht om (fysieke en logische) toegangsrechten van medewerkers te verwijderen bij een hernieuwde taaktoewijzing of bij beëindiging van de arbeidsrelatie.

Als controlemaatregel worden fysieke en logische toegangsrechten regelmatig en met vaste tussenpozen opnieuw gevalideerd. De eigenaar/operator van de netwerkelementen of de faciliteit is verplicht om de hervalidatie van toegangsrechten van medewerkers samen met de betreffende toezichthoudende manager uit te voeren, om te garanderen dat de medewerkers in het bezit blijven van een legitieme zakelijke noodzaak voor de toegang.

Vertrouwelijkheid

Gevoelige informatie van de klant die samenhangt met het leveren en beheren van TUNIX-diensten krijgt dezelfde beveiliging als de eigen TUNIX-informatie, inclusief encryptie bij het opslaan of overbrengen naar onbetrouwbare netwerken.

Door TUNIX beheerde klantinformatie wordt verder beschermd door de eis aan onze medewerkers zich bij indiensttreding of daarna te binden aan een geheimhoudingsovereenkomst.



Beheer van de werkstationbeveiliging

Het beleid t.a.v. werkstationbeveiliging beschermt informatiedragers van TUNIX en klanten door middel van een serie processen, waaronder verificatie van toegang van medewerkers tot werkstations, antivirusbescherming op pc's en bescherming van geclassificeerde gegevens en draagbare bezittingen. Het beveiligen van pc's tijdens het gebruik wordt verder geregeld door de vereiste van opstartwachtwoorden en waar mogelijk hardeschijfwachtwoorden, en met wachtwoorden beschermde toetsenbord- of schermvergrendelingen die automatisch in werking treden bij inactiviteit. Het management bij TUNIX is ervoor verantwoordelijk dat aan dit beleid wordt voldaan.

Alle TUNIX-werkstations dienen actieve en up-to-date antivirussoftware te hebben. TUNIX's leverancier van antivirussoftware levert regelmatig updates van virussignaturen die automatisch naar de werkstations worden verspreid. Bovendien voorzien de door de TUNIX Security Organization verspreide beveiligingsadviezen de TUNIX-medewerkers van informatie over viruswaarschuwingen, nieuwe beveiligingspatches en recent ontdekte kwetsbaarheden.

Controles op beveiligingsstatus en tests op kwetsbaarheid

TUNIX voert regelmatig tests en evaluaties uit om er zeker van te zijn dat beveiligingscontroles worden nageleefd en in overeenstemming met het beleid functioneren. Deze initiatieven omvatten de controle op beveiligingsstatus en de controle op kwetsbaarheid.

Proces van beveiligingsadviezen

TUNIX gebruikt een intern proces voor het vergaren en verspreiden van beveiligingsadviezen, gekoppeld aan nalevings- en beoordelingsprocessen als follow-up van deze adviezen. De adviezen komen van beveiligingsorganisaties uit de branche en van apparatuur- en systeemleveranciers. Ze bestaan voornamelijk uit recent geïdentificeerde gebreken in gevestigde netwerksoftware, -systemen en -apparatuur, waardoor niet-geautoriseerde gebruikers toegangscontroles zouden kunnen omzeilen en/of toegang tot gegevens zouden kunnen krijgen. Voor alle beheerde componenten houdt TUNIX aankondigingen van leveranciers en organisaties zoals CERT m.b.t. beveiligingspatches en kwetsbaarheden voortdurend in de gaten. De processen t.a.v. adviezen en integriteit van de beveiliging garanderen dat beveiligingspatches tijdig op de netwerksystemen worden toegepast. Elk beveiligingsadvies wordt gecategoriseerd en krijgt van de TUNIX Security Organization een ernstgraad, die op zijn beurt de periode bepaalt waarbinnen de kwetsbaarheid moet worden opgelost.



Rapportage en beheer van beveiligingsincidenten

TUNIX gebruikt een proces om beveiligingsincidenten en -bedreigingen tijdig te identificeren, het verlies of in gevaar komen van informatiedragers van TUNIX of onze klanten te minimaliseren en de oplossing van het incident te vergemakkelijken.

De netwerkexploitatiecentra van TUNIX voeren 24 uur per dag, 7 dagen per week realtime beveiligingsmonitoring uit op de netwerken van TUNIX en zijn klanten om beveiligingsincidenten te onderzoeken, ernaar te handelen en te reageren. Een deel van ons programma voor beveiligingsmonitoring omvat proactieve inspanningen op basis van trends en analyses.

Netwerkgerelateerde beveiligingsincidenten zouden invloed kunnen hebben op netwerkdiensten die TUNIX levert aan TUNIX-entiteiten (volledig eigendom van TUNIX, onder contract of partnerentiteiten) en TUNIX-klanten. Bij het optreden van een beveiligingsincident stelt TUNIX de mate van potentiële invloed vast en informeert het de klanten als die gevaar lopen. Incidenten worden dagelijks aan het leidinggevende management gerapporteerd om aandacht te vestigen op de soorten aanvallen die door ons reactieteam worden gemeld, en op andere belangrijke informatie over incidenten en kwetsbaarheden.

Rapportage over de beveiligingsstatus

Informatie betreffende de beveiligingsstatus van TUNIX's infrastructuur en diensten wordt beheerd en gecommuniceerd op basis van wie belang heeft bij die informatie. De resultaten van beveiligingscontroles en kwetsbaarheidstests worden gevolgd en gerapporteerd door de beveiligingsprogramma's die verantwoordelijk zijn voor het beheer van de naleving van die activiteiten. De huidige status wordt op cumulatieve basis gedeeld met het TUNIX management. De beveiligingsstatus en de voortgang bij beveiligingsinitiatieven wordt gerapporteerd aan de beveiligingsfunctionaris.

Beoordeling van het naleven van de beveiliging

TUNIX beschouwt beveiligingsbeoordelingen als essentieel voor het evalueren van de naleving van de ingestelde beveiligingsprocedures. De resultaten van deze beoordelingen worden gerapporteerd aan de directie.

Beveiligingsbeoordelingen worden samengesteld uit de volgende elementen:

- een beoordeling van de lokale netwerkinfrastructuur en kwetsbaarheidsscans van de netwerkcomponenten en beoordeelde toepassingen;



- een beoordeling van huidige beveiligingsprocessen en documentatie;
- een analyse van acties en verbeteringsplannen, en aanbevelingen voor verbeteringen van de beveiliging;
- een follow-up voor de uitvoering van verbeterplannen;
- het rapporteren van de resultaten aan de directie.

Bescherming van de netwerkperimeter

Alle externe netwerkverbindingen van TUNIX worden beschermd door firewalls die het binnenkomende en uitgaande verkeer screenen op basis van bron- en bestemmingsadres, protocol en poort, in overeenstemming met het veiligheidsbeleid. In het bijzonder worden internetverbindingen en extranetten beschermd door firewalls en DMZ'en die elke rechtstreekse netwerkroutering tussen het internet en interne TUNIX-netwerken blokkeren. Verbindingen van IP-netwerken van klanten met TUNIX-beheerfaciliteiten worden beschermd door toegangscontroles (zoals ACL's en firewalls) die binnenkomende en uitgaande pakketten screenen en alleen geautoriseerd verkeer doorlaten.

Detectie van inbraakpogingen

TUNIX maakt gebruik van instrumenten die elke poging van niet-geautoriseerde medewerkers tot het binnendringen in TUNIX-netwerkcomponenten detecteert. TUNIX zal klanten direct via het netwerkexploitatiecentrum inlichten als de indruk bestaat dat een gedetecteerde inbraakpoging de diensten bij de klant kan beïnvloeden.

Strategie van voortdurende verbetering

De wereld van netwerkbeveiliging verandert snel en is heel dynamisch: TUNIX verbetert de beveiliging voortdurend door middel van actieve onderzoeks- en ontwikkelingsprogramma's, het volgen van ontwikkelingen in de branche en het evalueren van nieuwe beveiligingstechnologieën en -producten. Nieuwe instrumenten worden toegepast op basis van een kosten-batenanalyse; de geselecteerde instrumenten en systemen zijn juist die, die effectieve beveiligingswaarborgen bieden.



5. Beveiligingsbewustzijn en -educatie

De TUNIX Security Organization is belast met het leiding geven aan en coördineren van beveiligingsbewustzijn en -educatie. De tweemaandelijks* vergadering en nieuwsbrief van TUNIX hebben een speciaal beveiligingsonderdeel. Voor het ontwikkelen van de inhoud hiervan maakt het programma gebruik van experts op het vakgebied uit de diverse beveiligingsprogramma's en -disciplines van de TUNIX educatie- en opleidingsorganisatie.

Beveiligingsopleiding en certificering

TUNIX moedigt zijn medewerkers aan beveiligingsopleidingen te volbrengen en accreditaties en certificeringen te behalen. Deze opleidingen worden zowel binnen TUNIX gegeven als door opleidingsorganisaties zoals:

- The International Information Systems Security Certification Consortium, Inc.((ISC) 2);
- The SANS Institute;
- Producent- en productspecifieke opleidingen en certificeringen, zoals Cisco, Microsoft, Tippingpoint, F5 en andere.



6. Ondernemingscontinuïteit & herstel na calamiteiten

TUNIX biedt expertise op het gebied van technische ondersteuning en programmabeheer die zich richt op het netwerkgedeelte van ondernemingscontinuïteit, beveiliging tegen calamiteiten en beheerde beveiligingsbehoeften van zowel TUNIX als haar klanten. TUNIX concentreert zich op alle aspecten van ondernemingscontinuïteit die nodig zijn om de ondernemingsprocessen te beschermen: beschikbaarheid, betrouwbaarheid, schaalbaarheid, herstelbaarheid, prestaties en beveiliging ten aanzien van netwerkinrichting. In samenwerking met de klant komt TUNIX tot een grondig inzicht in de behoeften van de onderneming en past het zijn kennis, expertise en bewezen methodologieën toe voor het implementeren van oplossingen op maat.

TUNIX-netwerken en -diensten worden ontworpen met een mate aan redundantie en herstelmogelijkheden die voldoet aan de overeengekomen Service Level Agreements. Voor unieke behoeften van klanten kunnen aan de hand van specifieke contractuele overeenkomsten aangepaste oplossingen met een extra hoog redundantieniveau worden gerealiseerd.

Calamiteiten kunnen chaos, onrust en verdriet veroorzaken, maar doen geen afbreuk aan TUNIX engagement met de klant. TUNIX weet dat wanneer de onderneming van de klant door een catastrofe wordt getroffen, een snel herstel van de communicatie essentieel is.



7. Beveiligingsverantwoordelijkheden van de klant

TUNIX-klanten zijn verantwoordelijk voor het beschermen van de beveiliging van hun onderneming, hun gegevens en de verbinding met het TUNIX-netwerk tegen verlies, openbaring, ongeoorloofde toegang of ontwrichting van de diensten. De klant dient TUNIX direct op de hoogte te brengen van elk op onze diensten betrekking hebbend werkelijk of vermoed beveiligingsincident waarvan hij gewaar wordt (bijvoorbeeld een directe melding als een klant denkt dat een niet-geautoriseerde partij toegang heeft verkregen tot zijn gebruikersidentificaties en -wachtwoorden, persoonlijke identificatienummers of kenmerken). De klant dient een beveiligingsbeleid te hebben vastgesteld en een functionerend beveiligingsprogramma te hebben om het beleid te ondersteunen. Het programma dient zich ten minste bezig te houden met fysieke en logische beveiliging en de vertrouwelijkheid van gegevens. De klant dient een lid van het management aan te stellen als eigenaar van zijn beveiligingsbeleid en -programma. De beveiligingsplichten van de klant omvatten, maar zijn niet beperkt tot:

- de verantwoordelijkheid voor het beschermen van de vertrouwelijke informatie van de klant tegen openbaring, en het beheer van gegevens, inhoud en transactie-informatie van de klant die is opgeslagen op of wordt overgebracht via het TUNIX-netwerk (bijvoorbeeld het back-uppen of herstellen van gegevens en het wissen van gegevens van schijfruimte die de klant beheert);
- de verantwoordelijkheid voor het selecteren en toepassen van de geschikte diensten en beveiligingskenmerken en -opties die voldoen aan de zakelijke en beveiligingsbehoeften van de klant, zoals bescherming van de privacy van persoonlijke informatie;
- de verantwoordelijkheid voor het ontwikkelen en handhaven van geschikte beheer- en beveiligingsprocedures zoals regelingen en processen voor fysieke en logische toegang (bijvoorbeeld beveiliging van het aanmelden bij toepassingen, inclusief unieke gebruikersidentificaties en wachtwoorden/pincodes/kenmerken die voldoen aan behoudzame beveiligingsnormen) op alle door de klant voorziene en beheerde netwerkapparatuur en -systemen;
- de verantwoordelijkheid voor de fysieke beveiliging van apparaten en systemen op het terrein van de klant, inclusief het voorkomen van het installeren van ongeoorloofde sensoren, sniffers en af luisterapparatuur op het terrein van de klant;
- de verantwoordelijkheid ervoor te zorgen dat zijn eindgebruikers voldoen aan de toepasselijke wetgeving en de Acceptable Use Policy voor ondernemingen (zie bijvoorbeeld <http://www.cbppweb.nl>);



- de verantwoordelijkheid voor de gedragingen en nalatigheden van de eindgebruikers van de klant m.b.t. enige bij TUNIX verkregen dienst; de verantwoordelijkheid om TUNIX direct in te lichten over enige inbreuk op de beveiliging die door de klant met betrekking tot de door TUNIX geleverde diensten wordt ontdekt.

Veel nationale wetgeving verbiedt het zich heimelijk toegang verschaffen tot gegevens die worden overgedragen via een openbaar netwerk of commerciële carrier (bijvoorbeeld internet) en onbeveiligde transmissielijnen (bijvoorbeeld gsm, radio of satelliet). Deze open transmissiediensten bieden echter wel betere mogelijkheden om op een heimelijke manier overgedragen gegevens te verkrijgen. Daarom dient al het vertrouwelijke verkeer bij overdracht via dergelijke netwerken of lijnen te worden versleuteld; dit is de verantwoordelijkheid van de eigenaar van de gegevens.

