netwerkbeveiligings-beleid

Sjabloon

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole** |  |
| Auteur |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door |  |
| Laatste herzieningsdatum |  |

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum van goedkeuring** | **Goedgekeurd door** | **Beschrijving van verandering** |
| 1.0 |  |  |  |

# Intro

Netwerkbeveiliging binnen de organisatie is belangrijk omdat het je eerste verdediging is tegen aanvallen van buitenaf. Door effectieve technische en organisatorische maatregelen voor netwerkbeveiliging te implementeren, kun je voorkomen dat cybercriminelen je infrastructuur in kaart brengen, je communicatie verstoren, onrechtmatig data vergaren of kritieke toepassingen en apparaten bereiken.

Dit beleidsdocument maakt deel uit van een set van beleidsdocumenten die **[Organisatie]** ondersteunen bij het opstellen van een gedegen strategie rond cyberbeveiliging.

# Netwerkbeveiliging

## Fysieke beveiliging

Netwerkcomponenten zoals firewalls en switchen moeten zich in speciale kasten bevinden. Toegang tot deze kasten moet worden beperkt tot speciaal daarvoor aangewezen personeel. Data- en stroomkabels moeten worden beschermd tegen beschadiging.

## Segregatie van netwerken

Om te voorkomen dat malware en ander misbruik zich over het netwerk verspreidt, moet het netwerk worden ontworpen als een gescheiden topologie. Systemen moeten zich in aangewezen VLAN's bevinden, gescheiden door firewall toegangsregels.

De volgende VLAN segregatieregels moeten in acht worden genomen:

* Systemen die online diensten leveren (d.w.z. inkomend verkeer van het internet accepteren) moeten worden gescheiden van andere systemen.
* Netwerkmanagement verloopt via een afzonderlijke VLAN.
* Systemen die verbonden diensten leveren (d.w.z. inkomend verkeer accepteren van niet vertrouwde netwerken anders dan het internet) moeten worden gescheiden van andere systemen
* Eindgebruikersapparaten moeten worden gescheiden van servers.
* Onbeheerde apparaten moeten worden gescheiden van beheerde apparaten.
* Systemen met verschillende doeleinden moeten van elkaar worden gescheiden.
* Fysieke locaties moeten van elkaar gescheiden zijn.
* Ontwikkelings-, test- en productiesystemen moeten van elkaar gescheiden zijn.

## Firewalling

VLAN's moeten worden gescheiden door firewalls. Netwerkverkeer tussen VLAN's en verkeer van of naar niet-vertrouwde netwerken moet worden geblokkeerd, tenzij het expliciet open moet zijn. Uitgaande internettoegang voor VLAN's van kantoorgebruikers is toegestaan, tenzij dit een negatieve invloed heeft op de beveiliging of prestaties van het bedrijf. Verkeer kan worden geprioriteerd, bijvoorbeeld om te voorkomen dat video- of muziekstreams het werk gerelateerde kantoorverkeer beïnvloeden.

## VPN

Voor telewerken of machine-naar-machine communicatie over onvertrouwde netwerken kan VPN gebruikt worden om netwerkverkeer te versleutelen dat standaard niet versleuteld is.

De toegang tot de VPN en dus tot alle achterliggende **[Organisatie]** systemen, moet waar mogelijk geconfigureerd zijn om gebruik te maken van een vorm van Multi Factor Authenticatie zodanig dat een niet bevoegd persoon die in het bezit is van gecompromitteerde **[Organisatie]** credentials geen gebruik kan maken van het **[Organisatie]** VPN.

## Beveiliging van bekabelde netwerken

# Netwerkpoorten moeten beschermd worden tegen niet-vertrouwde apparaten. Wanneer de fysieke beveiliging laag is, moeten netwerkbeveiligingstechnieken zoals MAC-filtering of netwerktoegangsbeveiliging gebruikt worden om niet-vertrouwde apparaten te blokkeren of te isoleren.

## Draadloze netwerkbeveiliging

Wifi gebruikt verschillende standaarden voor encryptie en verificatie. Hieronder staan de methoden in volgorde van beste beveiliging (de eerste is de enige veilige methode):

1. WPA2 + AES
2. WPA + AES (niet de voorkeur)
3. WPA + TKIP (niet de voorkeur)
4. WEP (nooit gebruiken)
5. Open Netwerk (nooit gebruiken)

Gebruikerstoegang moet worden gecontroleerd. Voor de verificatie van WIFI-netwerken wordt de voorkeur gegeven aan een centrale gebruikersdatabase op naam. De meeste zakelijke Wifi access points bieden LDAP- of RADIUS-ondersteuning.   
Onbeheerde toestellen mogen enkel toegang krijgen tot **[speciale WIFI netwerken voor gasten].** Netwerkverkeer tussen gastnetwerken en de door **[Organisatie]** beheerde netwerken moet worden voorkomen.

# Netwerkbeheer

* Er wordt een high-level netwerkschema ontwikkeld en (afgedrukt) veilig opgeslagen. Dit schema omvat de hardware- en functie omschrijving, alsook de nodige (IP) adressering. Dit schema wordt op regelmatige basis bijgewerkt.
* De managementpoorten moeten beperkt worden tot bevoegd personeel en mogen niet verbonden zijn met het internet, tenzij via VPN.
* Gebruikerstoegang tot beheerpoorten moet regelmatig gecontroleerd worden. Een centrale gebruikersdatabase op naam verdient de voorkeur voor de authenticatie van de beheertoegang.
* Installatie of wijziging van netwerktoestellen moet gebeuren door of in samenspraak met **[Organisatie]** IT.
* Netwerkinfrastructuur-apparaten zijn voorzien van logging, waarbij wordt gefocust op het monitoren en controleren van verkeersstromen via netwerkzones en verschillende vertrouwensniveaus. Voorbeelden hiervan zijn belangrijke beheerdergebeurtenissen zoals aanmelden, systeemaanpassingen, wachtwoord resetten…
* Om de beschikbaarheid en prestaties van kritieke en vertrouwelijke systemen te garanderen dient er gekeken te worden naar de aanwezigheid van service level agreements (SLA’s) voor deze netwerkcomponenten.