

CASUS RISICOMANAGEMENT



Opleiding:	Cybersecurity AD
Vak/Semester	Risicomanagement
Blok	3
Doelgroep:	Docenten
Auteur:	Wicky Ramrattan Msc.
Versie:	1.0
Datum:	12-01-2026
Classificatie:	Hogeschool van Amsterdam intern – docenten & studenten

Inhoud

1. Organisatiecontext	3
2. Digitale Infrastructuur en informatievoorziening	4
Elektronisch Zorg- en Patiëntendossier (EZPD)	4
Digitale Leer- en Samenwerkingsomgeving (DLO)	4
Medische apparatuur en zorgtechnologie (IoT)	4
Zorgplatform Vanguard Connect	5
HR & Planning	5
Financiën & Declaraties	6
Netwerkinfrastructuur	6
3. Bedrijfsprocessen	16
Zorgverlening en patiëntbehandeling	16
Administratie, planning en facturatie	16
Samenwerking met externe partijen	16
4. Mensen & organisatie	17
Medewerkers en gedrag	17
IT-organisatie en governance	17
5. Incidenten, waarschuwingssignalen en auditobservaties	18
6. Wet- en normenkader	19
7. Opdracht aan de Information Security Officers	20

1. Organisatiecontext

Vanguard Healthcare is een middelgrote Nederlandse zorgorganisatie die gespecialiseerde zorg levert binnen de regio Randstad en Midden-Nederland. De organisatie richt zich op acute zorg, chronische zorg en diagnostische dienstverlening en combineert ziekenhuiszorg met poliklinische zorg en digitale zorg op afstand.

Vanguard Healthcare bestaat uit:

- Twee algemene ziekenhuizen
- Vijf poliklinische behandelcentra
- Een digitaal zorgplatform(Vanguard Connect) voor thuiszorg en e-consulten

De organisatie telt ongeveer 1.100 medewerkers, waaronder artsen, verpleegkundigen, zorgcoördinatoren, administratief personeel, IT-specialisten en externe zorgprofessionals. Daarnaast werkt Vanguard Healthcare samen met opleidingsinstituten, waardoor stagiairs en zorgstudenten toegang krijgen tot interne leer- en informatiesystemen.

Jaarlijks verwerkt Vanguard Healthcare gegevens van ruim 150.000 patiënten. Deze gegevens omvatten medische dossiers, behandelplannen, medicatiegegevens, lab-resultaten, beeldmateriaal en communicatie tussen zorgverlener en patiënt. Deze informatie behoort tot bijzondere persoonsgegevens en vereist een hoog niveau van vertrouwelijkheid, integriteit en beschikbaarheid.

2. Digitale Infrastructuur en informatievoorziening

Elektronisch Zorg- en Patiëntendossier (EZPD)

Het primaire informatiesysteem binnen Vanguard Healthcare is het Elektronisch Zorg- en Patiëntendossier (EZPD). Dit systeem wordt gehost in een hybride cloudomgeving, waarbij een externe leverancier verantwoordelijk is voor hosting, onderhoud en updates.

Het EZPD wordt gebruikt voor:

- Vastleggen en raadplegen van patiëntgegevens
- Medicatiebeheer
- Diagnostiek en behandelplannen
- Communicatie met externe zorgpartners (zoals laboratoria)

Toegang tot het EZPD verloopt via gebruikersaccounts met rol gebaseerde autorisaties. Interne medewerkers loggen in via het interne netwerk; externe zorgprofessionals maken gebruik van een VPN-verbinding. Multi-factor authenticatie is geïmplementeerd voor beheerders, maar nog niet organisatie breed afgedwongen.

Digitale Leer- en Samenwerkingsomgeving (DLO)

Vanguard Healthcare beschikt over een Digitale Leeromgeving (DLO) voor:

- Opleiding en bijscholing van zorgpersoneel
- Stageopdrachten en reflectieverslagen
- Kennisdeling tussen afdelingen

In de DLO worden regelmatig casussen gebruikt die zijn gebaseerd op echte zorgsituaties. Hoewel deze casussen bedoeld zijn om geanonimiseerd te zijn, blijkt in de praktijk dat in reflectieverslagen soms indirect herleidbare patiëntinformatie wordt opgenomen.

Autorisaties binnen de DLO zijn niet altijd actueel, waardoor er risico bestaat op ongewenste inzage tussen gebruikersgroepen.

Medische apparatuur en zorgtechnologie (IoT)

Binnen Vanguard Healthcare wordt intensief gebruikgemaakt van medische apparatuur die gekoppeld is aan het netwerk, waaronder:

- Infuuspompen
- Patiëntmonitoringssystemen
- Mobiele diagnostische apparatuur
- Thuiszorgapparatuur die data doorstuurt naar het EZPD

Een deel van deze apparatuur draait op verouderde software en ontvangt niet structureel beveiligingsupdates. De apparatuur is functioneel noodzakelijk voor zorgverlening, maar vormt tegelijkertijd een potentieel aanvalsvlak binnen de IT-infrastructuur.

Vanguard Healthcare heeft recent een slimme verlichtingsoplossing geïmplementeerd op de spoedeisende hulp (SEH) en intensive care-afdelingen (ICU). De verlichting wordt centraal aangestuurd via een PLC-systeem dat verbonden is met sensoren, tijdschema's en een HMI-dashboard.

Zorgplatform Vanguard Connect

Vanguard Healthcare maakt gebruik van het digitale zorgplatform Vanguard Connect, dat fungeert als het primaire patiëntenportaal. Via dit platform kunnen patiënten onder andere:

- e-consults aanvragen en voeren met zorgverleners,
- medische uitslagen inzien,
- berichten uitwisselen met artsen en verpleegkundigen,
- afspraken beheren en notificaties ontvangen.

Vanguard Connect is een Cloud gebaseerde webapplicatie die toegankelijk is via internet en gekoppeld is aan het Elektronisch Zorg- en Patiëntendossier (EZPD) via API-koppelingen (o.a. REST/FHIR). Authenticatie van patiënten vindt plaats via een eigen accountstructuur met aanvullende verificatiemechanismen, terwijl zorgverleners authenticeren via de federatie met Azure Active Directory.

Het platform verwerkt zowel persoonsgegevens als bijzondere medische gegevens en vormt daarmee een kritisch informatiekanaal tussen patiënt en zorgorganisatie.

De beschikbaarheid van Vanguard Connect is belangrijk voor de continuïteit van zorg op afstand. Het platform is direct aan het internet blootgesteld.

HR & Planning

Voor personeelsbeheer maakt Vanguard Healthcare gebruik van een Cloud gebaseerde HR- en planningsapplicatie. Dit systeem ondersteunt:

- roosterplanning voor zorgmedewerkers,
- registratie van gewerkte uren,
- verlofaanvragen en beschikbaarheid,
- koppelingen met salarisverwerking.

De HR & Planning-applicatie is geïntegreerd met het identity management van Vanguard Healthcare, waardoor gebruikersaccounts worden aangemaakt op basis van functie en rol. In de praktijk blijken autorisaties sterk afhankelijk van correcte invoer van functies en tijdige verwerking van functiewijzigingen, zoals interne overplaatsingen of het beëindigen van tijdelijke contracten.

De HR & Planning-applicatie bevat de volgende gegevens van medewerkers:

- personeelsnummers,
- contractgegevens,
- werktijden en beschikbaarheid.

Financiën & Declaraties

De financiële afhandeling van zorgverlening binnen Vanguard Healthcare verloopt grotendeels digitaal via een financieel systeem voor declaraties en facturatie, dat gekoppeld is aan zorgverzekeraars. Dit systeem ontvangt gegevens vanuit het EZPD over geleverde zorg, behandelingen en verrichtingen, en vertaalt deze naar declaraties richting externe partijen.

De uitwisseling van declaratiegegevens vindt plaats via:

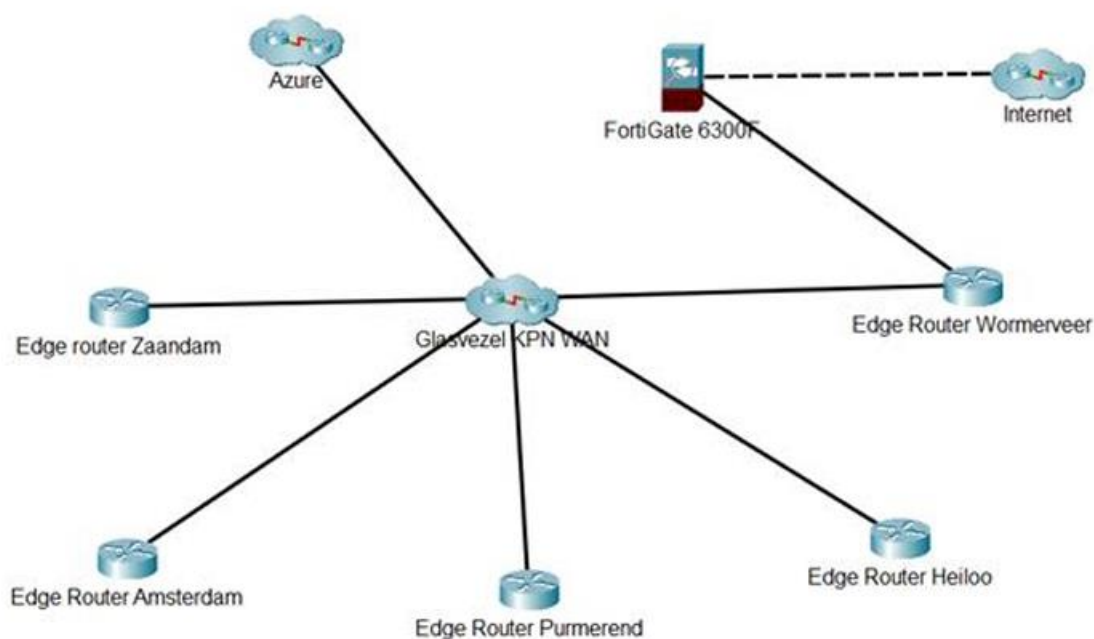
- beveiligde API-koppelingen,
- EDI- of SFTP-verbindingen,
- periodieke batchverwerkingen.

Het systeem verwerkt zowel financiële gegevens als zorg gerelateerde metadata.

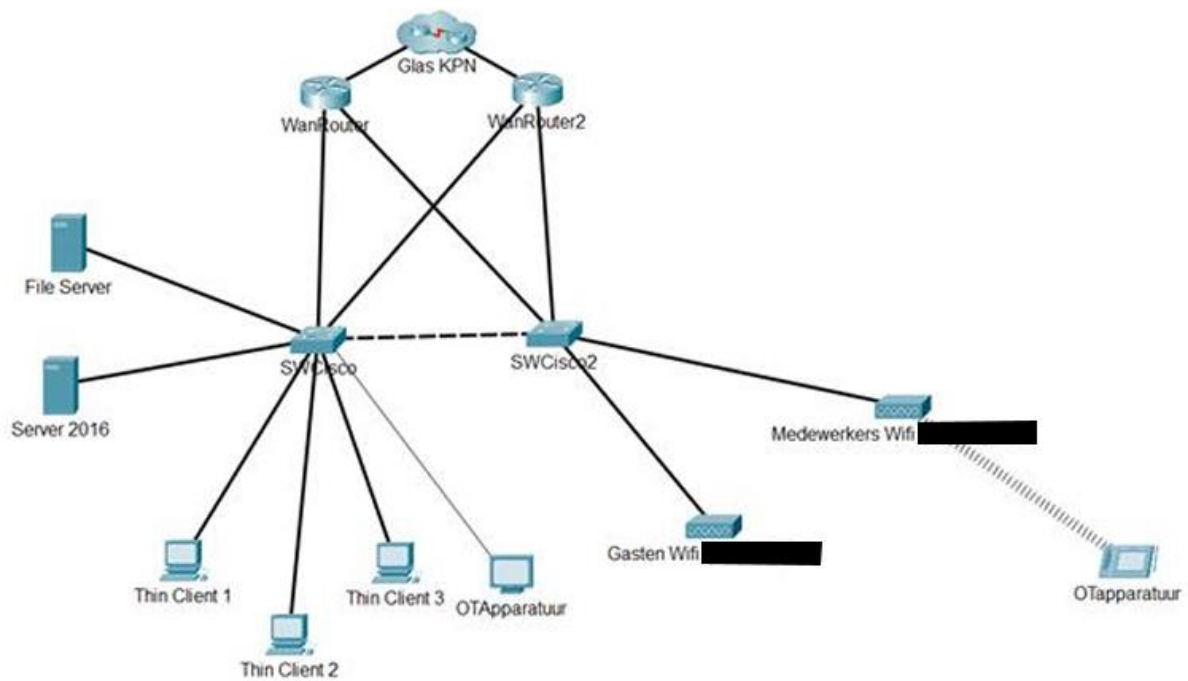
Netwerkinfrastructuur

maakt gebruik van een breed opgezet netwerk dat meerdere locaties met elkaar verbindt via een glasvezel KPN WAN.

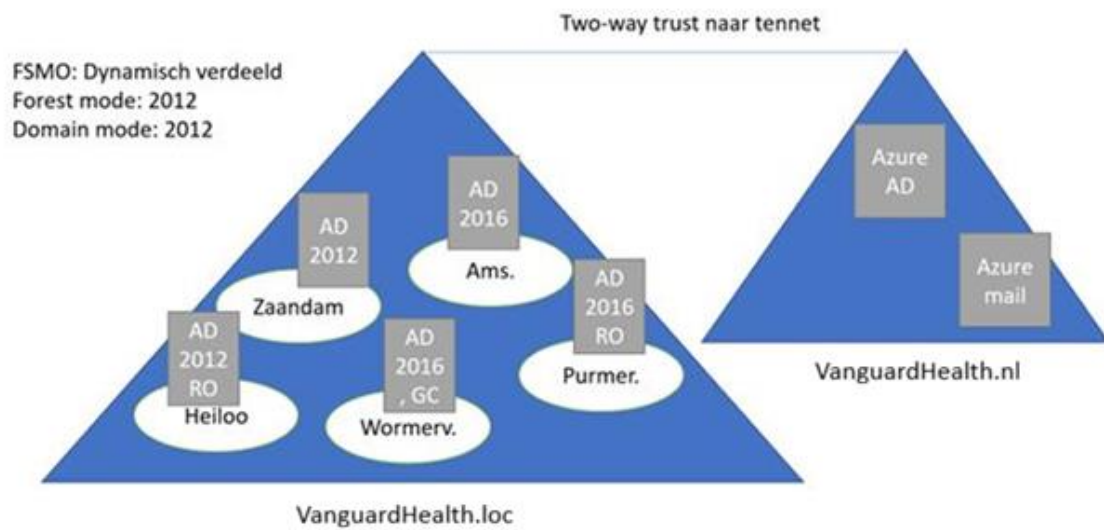
Topologie



Lokale topologie



AD-Infrastructuur



Overzicht van de IT-infrastructuur per locatie

Device	Vestiging	Ruimte	Omschrijving
SRV	Amsterdam	Serverruimte	VMWARE ESXI Hypervisor 6.5. 20 Server VM's (o.a. OT aansturing)
SRV	Amsterdam	Serverruimte	Windows Server 2016, AD, DHCP, DNS, GPO
SRV	Amsterdam	Serverruimte	Vmware Horizon 7.2, VDI infrastructuur
SRV	Amsterdam	Serverruimte	File Server, Debian, Rsync implementatie
Switch	Amsterdam	Serverruimte, Patchruimtes	Juniper EX Switches, 20 stuks, 2300XT, Vlan, Voice Vlan,
End devices	Amsterdam	Kantoren	Thin clients, Vmware horizon clients, Authenticatie op AD, Windows 10
End devices	Amsterdam	Medische apparatuur	Verschillende leveranciers, Windows Embedded 8.1 meestal, OT omgeving over TCP
Router	Amsterdam	Serverruimte	Onderdeel van collapsed core, 2 stuks, VRRP, OSPF, GRE tunnel over glasvezel
SRV	Zaandam	Serverruimte	VMWARE ESXI Hypervisor 7. 10 Server VM's (o.a. OT aansturing)

SRV	Zaandam	Serverruimte	Windows Server 2012, AD, DHCP, DNS, GPO
SRV	Zaandam	Serverruimte	Vmware Horizon 7.2, VDI infrastructuur
SRV	Zaandam	Serverruimte	File Server, Debian, Rsync implementatie
Switch	Zaandam	Serverruimte, Patchruimtes	Cisco 2960-X switches, 10 stuks, 15, Vlan, Voice Vlan, IOS 15.2
End devices	Zaandam	Kantoren	Thin clients, Vmware horizon clients, Authenticatie op AD, Windows 10
End devices	Zaandam	Medische apparatuur	Verschillende leveranciers, Windows Embedded 8.1 meestal, OT omgeving over TCP
Router	Zaandam	Serverruimte	1 stuks, OSPF, GRE tunnel over glasvezel
SRV	Heiloo	Patchruimte	Windows Server 2012, AD RO, DHCP, DNS, GPO
SRV	Heiloo	Patchruimte	File Server, Debian, Rsync implementatie
Switch	Heiloo	Patchruimtes	Cisco 2960-X switches, 2 stuks, Vlan, Voice Vlan, WLAN vlan, IOS 15.2
End devices	Heiloo	Kantoren	Thin clients, Vmware horizon clients, Authenticatie op AD, Windows 10
End devices	Heiloo	Medische apparatuur	Verschillende leveranciers, Windows Embedded 8.1 meestal, OT omgeving over TCP
Router	Heiloo	Serverruimte	1 stuks, OSPF, GRE tunnel over glasvezel
SRV	Purmerend	Patchruimte	Windows Server 2016, AD RO, DHCP, DNS, GPO
SRV	Purmerend	Patchruimte	File Server, Debian, Rsync implementatie
Switch	Purmerend	Patchruimtes	Cisco 2960-X switches, 2 stuks, Vlan, Voice Vlan, WLAN vlan, IOS 15.2

End devices	Purmerend	Kantoren	Thin clients, Vmware horizon clients, Authenticatie op AD, Windows 10
End devices	Purmerend	Medische apparatuur	Verskillende leveranciers, Windows Embedded 8.1 meestal, OT omgeving over TCP
Router	Purmerend	Serverruimte	2 stuks, VRRP, OSPF, GRE tunnel over glasvezel
SRV	Wormerveer	Serverruimte	Windows Server 2016, DHCP, DNS, GPO, Koppeling met Azure AD tennet (office 365 implementatie voor email)
SRV	Wormerveer	Serverruimte	File Server, Debian, Rsync implementatie
NGFW	Wormerveer	Serverruimte	FortiGate 6300F
Switch	Wormerveer	Patchruimte	Juniper EX Switches, 5 stuks, 2300XT, Vlan, Voice Vlan,
End devices	Wormerveer	Kantoren	Thin clients, Vmware horizon clients, Authenticatie op AD, Windows 10
End devices	Wormerveer	Medische apparatuur	Verskillende leveranciers, Windows Embedded 8.1 meestal, OT omgeving over TCP
Router	Wormerveer	Serverruimte	2 stuks, VRRP, OSPF, GRE tunnel over glasvezel

Router Zaandam

```
version 20.1R1.11;
system {
  root-authentication {
    plain-text-password "VandaagIsEchtBeter";
  }
}
interfaces {
  ge-0/0/0 {

    unit 0 {
      family inet {
        address 192.168.1.1/24;
      }
    }
  }
  ge-0/0/1 {
    unit 0 {
      family inet {
        address 192.168.2.1/24;
      }
    }
  }
  xe-0/0/0 {
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
  xe-0/0/1 {
    unit 0 {
      family inet {
        address 10.0.1.1/24;
      }
    }
  }
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface ge-0/0/0.0 {
        authentication {
          plain-text-password "VandaagBeter";
        }
      }
    }
    area 0.0.0.1 {
      interface ge-0/0/1.0 {
        authentication {
          plain-text-password "VandaagBeter";
        }
      }
    }
  }
  enable;
}
eigrp {
  router-id 192.168.3.1;
  interface xe-0/0/0.0 {
    passive;
  }
}
```

```

vrrp {
  group vrrp-group {
    virtual-address 192.168.1.254;
    priority 100;
    preempt;
    interface ge-0/0/0.0;
  }
}
}
interfaces {
  gr-0/0/0 {
    unit 0 {
      tunnel {
        source 10.0.0.1;
        destination 203.0.113.1;
      }
      family inet {
        address 192.168.4.1/30;
      }
    }
  }
}
system {
  services {
    telnet {
      listen {
        address 192.168.1.1;
      }
    }
  }
  login {
    user admin {
      class super-user;
      authentication {
        encrypted-password "$1$JfNKCvW$ql9jC1T6sQkxW7rlcMp1E/"; ## SECRET-DATA
      }
    }
  }
}
snmp {
  community public {
    authorization read-only;
  }
}
}

```

Switch Zaandam

```
## VLAN Configuration ##
show vlans
vlan10 {
  vlan-id 10;
  spanning-tree {
    stp;
    priority 61440;
  }
}
vlan20 {
  vlan-id 20;
  spanning-tree {
    stp;
    priority 61440;
  }
}
vlan30 {
  vlan-id 30;
  spanning-tree {
    stp;
    priority 61440;
  }
}
vlan40 {
  vlan-id 40;
  spanning-tree {
    stp;
    priority 61440;
  }
}
vlan50 {
  vlan-id 50;
  spanning-tree {
    stp;
    priority 61440;
  }
}
vlan60 {
  vlan-id 60;
  spanning-tree {
    stp;
    priority 61440;
  }
}
vlan70 {
  vlan-id 70;
  spanning-tree {
    stp;
    priority 61440;
  }
}
```

```

    }
}
vlan80 {
    vlan-id 80;
    spanning-tree {
        stp;
        priority 61440;
    }
}
vlan90 {
    vlan-id 90;
    spanning-tree {
        stp;
        priority 61440;
    }
}
vlan100 {
    vlan-id 100;
    spanning-tree {
        stp;
        priority 61440;
    }
}

## Interface Configuration ##
show interfaces
ge-0/0/0 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            native-vlan-id 1;
            native-vlan-id none;
            trunk {
                encapsulation flexible-ethernet-services;
            }
            dtp {
                interface-mode dynamic;
            }
        }
    }
}

ge-0/0/1 {
    unit 0 {
        family ethernet-switching {
            port-mode trunk;
            native-vlan-id 1;
            native-vlan-id none;
            trunk {
                encapsulation flexible-ethernet-services;
            }
        }
    }
}

```

```

        dtp {
            interface-mode dynamic;
        }
    }
}

## SNMP Configuration ##
show snmp
community public {
    authorization read-write;
}

## Telnet Configuration ##
show system services
telnet;

show system login
user admin {
    authentication {
        plaintext-password "VandaagGoed";
    }
    class super-user;
}

## Console Configuration ##
show system login
user admin {
    class super-user;
}

## System Configuration ##
show system
host-name SWZaandam;
last-reboot "2021-11-12";

```

3. Bedrijfsprocessen

Zorgverlening en patiëntbehandeling

Het kernproces van Vanguard Healthcare is het leveren van veilige, tijdige en kwalitatieve zorg. Zorgverleners zijn sterk afhankelijk van continue beschikbaarheid en betrouwbaarheid van digitale systemen. Verstoringen in IT-systemen kunnen directe gevolgen hebben voor:

- Medicatietoediening
- Diagnosestelling
- Overdracht van patiëntinformatie tussen afdelingen

Digitale verstoringen kunnen daarmee leiden tot directe risico's voor patiëntveiligheid.

Administratie, planning en facturatie

Ondersteunende processen zoals personeelsplanning, declaraties richting zorgverzekeraars en facturatie zijn sterk geautomatiseerd en gekoppeld aan het EZPD. Onjuistheden of dataverlies kunnen leiden tot:

- Financiële schade
- Onjuiste declaraties
- Reputatieschade richting zorgverzekeraars en toezichthouders

Samenwerking met externe partijen

Vanguard Healthcare werkt samen met diverse externe partijen, waaronder:

- Diagnostische laboratoria
- ICT- en Cloud leveranciers
- Softwareontwikkelaars
- Zorgverzekeraars

Gegevensuitwisseling vindt plaats via API-koppelingen, beveiligde portalen en e-mail. Contractuele afspraken over informatiebeveiliging en continuïteit zijn historisch gegroeid en niet altijd aantoonbaar afgestemd op actuele eisen vanuit NIS2 en de AVG.

4. Mensen & organisatie

Medewerkers en gedrag

Medewerkers binnen Vanguard Healthcare hebben verschillende niveaus van digitale vaardigheid. Hoewel er jaarlijks verplichte awareness-trainingen worden aangeboden, blijkt uit interne signalen dat:

- Wachtwoorden worden hergebruikt
- E-mails niet altijd kritisch worden beoordeeld
- Accounts niet altijd tijdig worden aangepast bij functiewijzigingen

De hoge werkdruk binnen de zorg leidt ertoe dat beveiligingsmaatregelen soms als hinderlijk worden ervaren, wat kan resulteren in het omzeilen van procedures.

IT-organisatie en governance

De IT-afdeling van Vanguard Healthcare is relatief klein en richt zich vooral op operationeel beheer. Er is:

- Geen volledig ingericht ISMS in overeenstemming met ISO 27001
- Geen structureel gedocumenteerd risicomanagementproces
- Beperkte monitoring op beveiligingsincidenten

Risicoanalyses worden incidenteel uitgevoerd, vaak reactief na een incident of externe audit.

5. Incidenten, waarschuwingssignalen en auditobservaties

In de afgelopen periode heeft Vanguard Healthcare te maken gehad met:

- Een phishing-incident waarbij inloggegevens van een zorgmedewerker zijn buitgemaakt
- Een tijdelijke onbeschikbaarheid van het EZPD door een storing bij de Cloud leverancier
- Onjuiste autorisaties binnen de DLO, waardoor medische-studenten toegang hadden tot elkaars documenten
- MFA is nog niet voor alle gebruikers verplicht.
- IT-team is klein en vooral operationeel.
- Accounts van oud-stagiairs zijn soms nog actief in de DLO
- VPN-toegang wordt niet standaard herzien per kwartaal
- De IT-afdeling focust zich op onderhoud, niet op beveiliging – Problemen worden vooral opgelost als ze optreden, maar er wordt weinig gedaan om aanvallen vooraf te voorkomen.
- Regels en afspraken worden niet altijd goed gevolgd – Er zijn Service Level Agreements (SLA's), maar deze worden niet effectief gebruikt om beveiligingsproblemen op te lossen.
- Het netwerk is een mix van oude en nieuwe systemen
- Een verpleegkundige klikte op een link en voerde inloggegevens in op een nepportaal.
- Cloudleverancier had netwerkissue, 2 uur downtime.
- Medische IoT-apparatuur zit op hetzelfde netwerksegment als werkplekken op sommige afdelingen.
- Back-ups van sommige systemen worden door leverancier beheerd; interne zichtbaarheid beperkt.
- Er zijn meldingen van ongewenste lichtfluctuaties tijdens kritieke zorgmomenten. Dit zou kunnen wijzen op een mogelijke Cyberaanval gericht op de PLC-infrastructuur.

Hoewel deze incidenten niet hebben geleid tot een formele melding bij de Autoriteit Persoonsgegevens, heeft het bestuur vastgesteld dat de organisatie onvoldoende aantoonbaar grip heeft op haar cyberrisico's. De Raad van Bestuur geeft aan: "We willen aantoonbaar in control zijn.

6. Wet- en normenkader

Gegevensverwerking & privacy

Binnen Vanguard Healthcare vinden de volgende gegevensverwerking plaats:

- Diagnoses, medicatie, labuitslagen (bijzondere persoonsgegevens)
- Identiteitsgegevens en contactinformatie
- Communicatie tussen patiënt en arts
- Loggegevens uit EZPD en Vanguard Connect

Tevens vindt er ook gegevensverwerking plaats met externe partijen:

- EZPD-cloudleverancier (hosting, beheer)
- Extern laboratorium (uitslagen via koppeling)
- Externe ICT-partner (netwerkbeheer “op afroep”)
- Leverancier van medische IoT-monitoring

Bestuurlijke druk

De Raad van Bestuur verwacht:

- Duidelijke risico's die aantoonbaar raken aan AVG en NIS2
- Leveranciersrisico's helder (contracten, continuïteit)
- Een aanpak die later auditbaar is

Vanguard Healthcare moet voldoen aan en rekening houden met:

- **AVG** – vanwege verwerking van bijzondere persoonsgegevens
- **NIS2** – als essentiële zorginstelling

Daarnaast wil de organisatie haar informatiebeveiliging structureren aan de hand van:

- **NEN 7510** – zorg specifieke informatiebeveiliging
- **ISO 27001 & ISO 27005** – ISMS en risicomanagement
- **NIST Cybersecurity Framework** – operationele cybersecurity

7. Opdracht aan de Information Security Officers

Het bestuur van Vanguard Healthcare vraagt jullie, als cybersecurityconsultants, om een volledig risicoassessment uit te voeren.

Jullie opdracht is om:

1. De cyberrisico's van Vanguard Healthcare in kaart te brengen
2. De risico's te analyseren binnen de vier lagen:
 - a. Mensen
 - b. Bedrijfsprocessen
 - c. Applicatie/Data/Informatie
 - d. IT-infrastructuur (inclusief PLC-infrastructuur)
3. Per risico vast te stellen:
 - a. Asset
 - b. Dreiging
 - c. Kwetsbaarheid
 - d. Impact (BIV + patiëntveiligheid)
 - e. Risiconiveau
4. Passende technische en organisatorische maatregelen te formuleren
5. De analyse te onderbouwen met relevante wetgeving en standaarden

Het eindproduct moet het bestuur inzicht geven in:

- De belangrijkste cyberrisico's
- De prioriteiten voor verbetering
- Een prioriteitenlijst met maatregelen
- Quick wins binnen 30 dagen
- Middellange termijn (3 maanden)
- Structurele verbeteringen (12 maanden)
- Hoe Vanguard Healthcare aantoonbaar kan voldoen aan wet- en regelgeving