Kennisnet

8 maatregelen om uw ict-infrastructuur te beveiligen

Een onveilige ict-infrastructuur kan een school ontregelen: geen internet, verstoorde lessen, leerlingen die cijfers aanpassen, medewerkers die geen salaris ontvangen of data die op straat liggen. Met deze 8 maatregelen beveiligt u uw ict-infrastructuur en verkleint u de risico's.

Per maatregel leest u welk risico u ermee voorkomt, hoe u de maatregel uitvoert en hoeveel tijd en geld het kost. De meeste maatregelen kunt u bij de interne ict-dienst of de ict-dienstenleverancier neerleggen.

Let op dat deze maatregelen de *Aanpak IBP* niet vervangen, maar een aanvulling daarop zijn. Ook kunt u het *toetsingskader IBP* gebruiken voor meer maatregelen om uw data te beschermen.

Maatregel 1

Breng devices in kaart

Devices binnen de school die verbonden zijn met het netwerk kunnen beveiligingslekken bevatten. Denk aan printers, beveiligingscamera's, VoIP-telefoons, laptops en desktops. Dit is een risico voor uw data, omdat kwaadwillenden via de devices toegang kunnen krijgen tot uw informatiesystemen.

Hoe

1. Breng alle beheerde en onbeheerde, met het netwerk verbonden, devices in kaart.
2. Zorg dat deze database up-to-date is. Houd voor beheerde devices de softwareversie bij en voorzie de devices altijd van de laatste beveiligingsupdates nadat deze getest zijn.
3. Zorg er ook voor dat er op het device niet met een standaard combinatie van gebruikersnaam/wachtwoord ingelogd kan worden, zoals admin/admin.
4. Zorg ervoor dat onbeheerde devices geen toegang hebben tot cruciale diensten of servers. Gebruik hier bijvoorbeeld VLAN's voor.

Tijd

Kosten

Maatregel 2

Houd overzicht over uw netwerkinfrastructuur

Een goed overzicht van de netwerkinfrastructuur – dit is apparatuur zoals firewall, switches, netwerk-aansluitingen en netwerkbekabeling – is onmisbaar om updates op apparatuur goed uit te voeren.

Hoe

1. Maak een overzicht van:
   - alle ruimtes
   - de netwerkaansluitingen in de ruimtes
   - het VLAN per netwerkaansluiting
   - welk apparaat op de netwerkaansluiting is aangesloten, zoals camera's, printers of computers
   - wat de status van de software van het apparaat is (versie, update mogelijk/noodzakelijk)
   - welke netwerkapparatuur gebruikt wordt, zoals routers, switches en wifi-componenten
2. Gebruik dit overzicht om ongebruikte openbare netwerkaansluitingen te deactiveren en de software op de aangesloten devices actueel te houden, na de gebruikelijke test-procedures.
3. Houd dit overzicht actueel, bijvoorbeeld met behulp van specifieke software die dit voor delen van het overzicht automatisch doet. Nagios is een goed open source systeem dat dit doet.

Tijd

Kosten

Maatregel 3

Houd zicht op accounts van infrastructuur componenten

Om toegang te krijgen tot computers, servers, netwerk-componenten, printers, beveiligingscamera's, VoIP-telefoons, laptops en desktops heeft u een account nodig. Er zijn 3 soorten accounts: gebruikersaccounts, gebruikers-accounts met extra privileges en administrator-accounts.

Om misbruik van accounts te voorkomen, bijvoorbeeld doordat data gelekt wordt of een apparaat of systeem verkeerd wordt ingesteld, kunt u de volgende maat-regelen nemen.

Hoe

1. Maak een overzicht van alle infrastructuur componenten binnen de school, door bijvoorbeeld de overzichten uit maatregel 1 en 2 te combineren.
2. Laat periodiek voor de infrastructuur componenten in kaart brengen welke accounts extra privileges of administrator-toegang hebben in een autorisatiematrix.
3. Zorg dat beheerders een eigen account op naam hebben en voorkom dat standaard admin accounts (zoals admin, administrator, root) gebruikt worden.
4. Beperk privileges waar mogelijk.
5. Verwijder ongebruikte accounts.
6. Zorg dat er bij uit-dienst procedures aandacht wordt besteed aan het inactief maken of verwijderen van accounts.
7. Zorg bij veranderende rollen van medewerkers dat hun privileges daarop worden aangepast.

Tijd

Kosten

Maatregel 4

Controleer de toegang van externen tot uw interne netwerk

In sommige gevallen hebben externe leveranciers toegang van buiten nodig tot het interne netwerk. Bijvoorbeeld voor het beheer van de alarminstallatie, het systeem van de kluisjes, de lift of het gebouw-beheersysteem. U vertrouwt erop dat zij uw data niet stelen, maar soms kunnen zij na afloop van de werkzaamheden nog steeds bij uw systemen. Dit kan een risico zijn voor uw data.

Hoe

1. Houd in een centrale administratie bij welke leveranciers toegang nodig hebben, met welk doel, en leg afspraken vast over wat de leverancier wel of niet mag met uw gegevens in de *verwerkersovereenkomst* met de leverancier.
2. Trek de toegang na de werkzaamheden in.
3. Zorg voor een veilige VPN-verbinding.

Tijd

Kosten

Maatregel 5

Verbind apparaten draadloos en scherm vrij toegankelijke fysieke netwerkaansluitingen af

Voor leerlingen en buitenstaanders zijn vrij toegankelijke fysieke netwerkaansluitingen in een schoolgebouw een makkelijk doelwit voor misbruik. Iemand kan zich toegang verschaffen tot een server of netwerkapparatuur en gegevens stelen of dataverkeer afluisteren. Voorkom dit door indien mogelijk vrij toegankelijke netwerkaansluitingen af te schermen en apparaten zoveel mogelijk draadloos te verbinden.

Hoe

1. Breng de fysieke netwerkaansluitingen in kaart.
2. Plaats ze indien mogelijk uit het zicht voor buitenstaanders en leerlingen.
3. Is dat geen optie? Beperk dan de netwerktoegang via die aansluiting op uw switches, zodat cruciale diensten of servers ontoegankelijk zijn. Gebruik hier bijvoorbeeld VLAN's of MAC-adres filtering voor.

Tijd

Kosten

Maatregel 6

Implementeer anti-DDoS maatregelen

DDoS-aanvallen verstoren de ict en alle daarvan afhankelijke werkzaamheden binnen de school door het versturen van meer verzoeken dan het systeem aankan. Leerlingen kunnen niet meer bij hun digitale leeromgeving, de website is onbereikbaar en digitale toetsen moeten op een ander moment hervat worden. Hoe voorkomt u een DDoS-aanval?

Hoe

DDoS-aanvallen zitten zo complex in elkaar dat er niet één manier is om dit te voorkomen. Gebruik het Wikiwijs arrangement *Denial of Service* op school voor diepgaande informatie over wat een DDoS-aanval is en hoe u hier zelf mee om kunt gaan.

U kunt ook bij uw internetprovider of ict-dienstverlener informeren naar hun mogelijkheden om DDoS-bescherming voor uw internetverbinding op te zetten. De dienst Veilig internet van de coöperatie SIVON biedt deze functionaliteit standaard.

Tijd*

Zelf: ⏳⏳⏳⏳

Internetprovider: ⏳

SIVON: ⏳

Kosten*

Zelf: €€

Internetprovider: €€€€€

SIVON: €

*Afhankelijk van of u dit zelf doet of door een externe partij

Maatregel 7

Implementeer anti-ransomware maatregelen

Ransomware is een plaag die moeilijk te bestrijden is. Een besmet mailtje kan de bestanden op uw computer en de netwerkschijven waar de gebruiker toegang toe heeft versleutelen, waardoor u ze niet meer kunt gebruiken. Zelfs het bezoeken van een besmette website is al genoeg om uw bestanden ontoegankelijk te maken. Toch kunt u verschillende maatregelen treffen om het risico te verkleinen.

Hoe

1. Zorg voor continue bewustwording onder uw gebruikers, bijvoorbeeld door ze met voorbeelden van 'foute mailtjes' kennis te laten maken.
2. Werk zoveel mogelijk met bestanden die online staan, bijvoorbeeld in de Google G Suite-omgeving of Microsoft Office 365-omgeving. Deze platformen zorgen ervoor dat in veel gevallen van ransomware de bestanden die daar staan opgeslagen niet versleuteld worden. Train uw medewerkers om op deze wijze te werken.
3. Maak back-ups van belangrijke bestanden, zoals configuratiebestanden van netwerk-apparatuur, servers en andere infrastructuur componenten. Maak deze backups op fysiek gescheiden media en test de herstelprocedures periodiek uit. Indien u uw infrastructuur componenten niet zelf in beheer heeft, leg deze eis dan vast in de SLA met de leverancier.
4. Installeer op alle computers altijd de laatste updates van het besturingssysteem, na de gebruikelijke testprocedure.
5. Gebruik up-to-date anti-virus en anti-ransomware software.
6. Met sommige cybersecurity verzekeringen kunt u uw organisatie verzekeren tegen geleden financiële schade.

Tijd

Kosten

Heeft u ondanks de getroffen maatregelen toch te maken met ransomware? Op de website *No More Ransom!* staan decryptie tools waarmee u versleutelde bestanden ontsleutelt zonder dat u hackers hoeft te betalen.

Maatregel 8

Versleutel data op devices

Wanneer data op een device staan, dan bestaat het risico dat deze bestanden in verkeerde handen vallen wanneer u het device verliest of wanneer het wordt gestolen. Ook zonder wachtwoord zijn de bestanden of login-gegevens van informatiesystemen er makkelijk af te halen. Om dit te voorkomen kunt u de data op uw device versleutelen, zodat het onmogelijk wordt deze gegevens er zonder wachtwoord af te halen.

Hoe

Versleutel de bestanden op beheerde devices en eis dit op Bring Your Own Devices (BYOD) van medewerkers.

- Voor Windows devices kunt u de ingebouwde Bitlocker gebruiken. Dit beheert u met Intune.
- Voor Macbooks kunt u hier FileVault voor gebruiken.
- Chromebooks, en recente iOS en Android apparaten zijn al standaard versleuteld. Controleer dit bij aanschaf of als ze in beheer worden genomen. Controleer dit steekproefsgewijs, want gebruikers kunnen deze versleuteling zelf weer uitzetten.

Tijd

Kosten

Colofon

8 maatregelen om uw ict-infrastructuur te beveiligen

Datum van uitgave
november 2019

Auteur(s)
Bas Roset, Kennisnet

Redactie / eindredactie
Juwan Mizouri, Kennisnet

Vormgeving
Corps / Delta3

Over Kennisnet
Goed onderwijs legt de basis voor leven, leren en werken en daagt leerlingen en studenten uit om het beste uit zichzelf te halen. Dat vraagt om onderwijs dat inspeelt op sociale, economische en technologische ontwikkelingen. Kennisnet ondersteunt besturen in het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo) bij een professionele inzet van ict en is voor scholen de gids en bouwer van het ict-fundament.

Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

kennisnet.nl

Kennisnet
Postbus 778
2700 AT Zoetermeer

T 0800 321 22 33
E support@kennisnet.nl
I kennisnet.nl