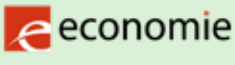
OFFICE~IT

SECTORGIDS

Bouwsector

De bouwsector vormt een essentiële pijler van onze economie en staat voor unieke cybersecurity-uitdagingen. Door de toenemende digitalisering van werven, het gebruik van slimme bouwtoepassingen en de samenwerking tussen tal van partners, onderaannemers en leveranciers, groeit ook de kwetsbaarheid voor digitale dreigingen.

Deze gids kwam tot stand met de steun van de FOD Economie en is gefinancierd door de Europese Unie & NextGenerationEU.



Digitale vooruitgang vraagt om gerichte cyberweerbaarheid!

Met deze reeks sectorgerichte gidsen willen we ondernemingen helpen om de kansen van digitalisering ten volle te benutten, zonder de gevaren van cyberdreigingen uit het oog te verliezen. Want wie vandaag digitaal onderneemt, moet ook digitaal weerbaar zijn.

We leven in een tijdperk waarin digitalisering niet langer optioneel is, maar essentieel om als onderneming mee te blijven draaien, te groeien en te innoveren. Technologie maakt onze bedrijven sneller, efficiënter en beter verbonden dan ooit tevoren. Van slimme toepassingen en cloud-oplossingen tot mobiele werkomgevingen en geautomatiseerde processen: digitalisering is de motor achter modern ondernemerschap.

Maar diezelfde digitalisering maakt bedrijven ook kwetsbaarder. Cyberdreigingen zijn de afgelopen jaren explosief toegenomen, in volume én in complexiteit. Cybercriminelen worden steeds professioneler en hun aanvallen steeds gerichter.

Geen enkele sector ontsnapt daaraan, en ook kleine en middelgrote ondernemingen worden steeds vaker het doelwit. Een phishingmail, een gehackte leverancier of een lek in verouderde software kan al voldoende zijn om volledige bedrijfsprocessen lam te leggen of gevoelige data bloot te stellen.

Cybersecurity is dus geen louter technisch verhaal meer, en al zeker geen zorg voor enkel de IT-afdeling. Het is een strategisch thema dat op elk niveau binnen de organisatie aandacht verdient, van de werkvloer tot het management. Want de impact van een cyberincident raakt alle lagen van het bedrijf: financieel, operationeel én reputatiegewijs.

Met deze sectorgidsen willen we bedrijven ondersteunen in hun zoektocht naar meer digitale weerbaarheid. Elke sector kent immers zijn eigen processen, kwetsbaarheden en digitale ecosystemen. Door cybersecurity sectorspecifiek te benaderen kunnen we praktischer adviseren, gerichter waarschuwen en effectiever oplossingen aanreiken.

Dit initiatief is in het leven geroepen om bewust-zijn rond cybersecurity te vergroten, maar vooral om actie te stimuleren. We willen ondernemingen helpen om niet alleen risico's te herkennen, maar ook de juiste stappen te zetten , van preventie tot reactie. Elke gids bevat daarom een combinatie van toegankelijke uitleg, realistische risico's en praktische aanbevelingen, afgestemd op de sector waarvoor ze is bedoeld.

Samen bouwen we zo aan een veerkrachtige, veilige en toekomstgerichte digitale economie, waarin ondernemers met vertrouwen kunnen blijven innoveren.

Cyberveiligheid in de bouw sector.

De bouwsector digitaliseert in snel tempo. Van digitale plannen en BIM-modellen tot online projectbeheer en slimme werfopvolging: technologie speelt vandaag een cruciale rol op elke werf. Maar die toenemende digitalisering maakt de sector ook kwetsbaarder voor cyberaanvallen. Van ransomware tot datadiefstal: de gevolgen van een succesvolle aanval kunnen zwaar wegen, met stilgelegde werven, financiële schade en reputatieverlies tot gevolg.

Ransomware-aanvallen

Bouwprojecten zijn vaak gebonden aan strikte tijdlijnen en budgetten. Ransomware-aanvallen kunnen leiden tot significante vertragingen en financiële verliezen doordat essentiële project-gegevens worden versleuteld en ontoegankelijk worden gemaakt.

Supply Chain-aanvallen

Bouwprojecten omvatten vaak een uitgebreide keten van leveranciers en subcontractors. Een zwakke schakel in deze keten kan een ingang zijn voor cybercriminelen om toegang te krijgen tot systemen en gevoelige informatie van het hele project.

Beveiliging van IoT-apparaten op de Bouwplaats

Moderne bouwplaatsen maken gebruik van IoT-apparaten (zoals slimme sensoren, GPS-apparaten, en bewakingssystemen). Deze apparaten zijn vaak kwetsbaar voor aanvallen, wat kan leiden tot verstoringen in bouwactiviteiten of het lekken van gevoelige gegevens.

Diefstal van Bouwplannen en IP

Bouwplannen, ontwerpen en andere intellectuele eigendommen zijn waardevol. Diefstal van deze informatie kan concurrentievoordeel geven aan rivalen of gebruikt worden voor kwaadaardige doeleinden.

Phishing en Social Engineering

Medewerkers in de bouwsector kunnen het doelwit zijn van phishing-aanvallen en social engineering tactieken, wat kan leiden tot ongeautoriseerde toegang tot systemen of financiële verliezen.

Verouderde Software en Systemen

De bouwsector maakt vaak gebruik van gespecialiseerde software voor project-management, ontwerp en communicatie. Deze software wordt niet altijd regelmatig bijgewerkt, waardoor kwetsbaarheden ontstaan.

Beveiliging van Mobiele Apparaten

Bouwprofessionals gebruiken vaak mobiele apparaten op locatie voor communicatie en toegang tot projectgegevens. Deze apparaten kunnen kwetsbaar zijn voor aanvallen als ze niet goed beveiligd zijn.

PRAKTISCHE MAATREGELEN

Regelmatige Beveiligingsupdates

Zorg ervoor dat alle software en systemen, inclusief IoT-apparaten, regelmatig worden bijgewerkt met de nieuwste beveiligingspatches.

Sterke Authenticatie en Toegangsbeheer

Implementeer multi-factor authenticatie en strikte toegangscontrole voor gevoelige gegevens en systemen.

Encryptie van Gegevens

Versleutel alle gevoelige informatie zowel in rust als tijdens overdracht om de impact van datalekken te minimaliseren.

Beveiligingsbewustzijn Training

Train medewerkers regelmatig in het herkennen van phishing-aanvallen en andere cyberdreigingen.

Beveiliging van IoT-apparaten

Zorg ervoor dat IoT-apparaten op de bouwplaats goed beveiligd zijn met sterke wachtwoorden en regelmatige firmware-updates.

Incident Response Plan

Ontwikkel en test een incident response plan om snel en effectief te kunnen reageren op cyber-incidenten.

Beveiliging van Mobiele Apparaten

Gebruik mobiele device management (MDM) oplossingen om de beveiliging van mobiele apparaten te waarborgen en verlies van gegevens te voorkomen.

Beveiliging van de Supply Chain

Werk samen met leveranciers en subcontractors om ervoor te zorgen dat ook zij voldoen aan de beveiligingsstandaarden. Dit kan door middel van audits, contractuele vereisten, en gezamenlijke beveiligingstrainingen.

Bouwstenen voor een succesvol én effectief cybersecuritybeleid

1 Inventariseren

Een doeltreffende cybersecurity start met een overzicht van alle hardware en software binnen je bedrijf.

2 Update

Regelmatige updates beschermen je systemen tegen kwetsbaarheden en zorgen voor een optimale veiligheid.

3 Multi-factor (MFA)

Met MFA bescherm je je accounts beter, zelfs als je wachtwoord wordt buitgemaakt.

4 Isoleren

Isolatie beperkt risico's door kwetsbare systemen los te koppelen van je netwerk.

5 Bewustzijn

Menselijke fouten blijven een groot cyberrisico, dus is bewustmaking cruciaal om veilig gedrag te stimuleren.

6 Anti-virus

Antivirussoftware vormt een essentiële eerste verdedigingslinie tegen malware en cyberaanvallen.

7 Toegang op afstand

Toegang op afstand biedt flexibiliteit, maar vraagt om sterke beveiliging om misbruik en datalekken te voorkomen.

8 Wargame

Een simulatie van een cyberaanval helpt je inschatten hoe goed je bent voorbereid op een echte digitale crisis.

UNIZO Podcasttip

De UNIZO Podcasts zijn er voor ondernemers die op zoek zijn naar inspiratie, inzichten en praktische tips, op het moment dat het hen past. Of je nu onderweg bent, tussen twee afspraken door wat tijd hebt of tijdens het werk even wil bijleren: de podcasts van UNIZO zijn jouw ideale compagnon.

Luister naar boeiende verhalen van collega-ondernemers, ontdek slimme strategieën en krijg advies van experten die weten wat er leeft in het ondernemerschap. Kort, krachtig en altijd relevant voor jouw zaak.

SPOTIFY **APPLE** **YOUTUBE**

1. Inventariseren

Een goede cybersecuritystrategie begint bij een helder overzicht van je digitale omgeving. Je kunt pas beschermen wat je kent. Daarom is het essentieel om eerst in kaart te brengen welke hardware en software je precies gebruikt binnen je onderneming. Die inventaris vormt de basis voor gerichte en efficiënte beveiligingsmaatregelen.

1 Wat?

Maak een lijst van alle hardware die binnen je onderneming aanwezig is, zoals pc's, servers, laptops, mobiele toestellen, NAS-schijven (harde schijven die autonoom verbonden zijn met je netwerk) en eventuele machines indien relevant.

Inventariseer de software die je gebruikt, inclusief zowel geïnstalleerde programma's op je pc's als web-based (cloud) toepassingen, en vermeld daarbij ook de software die je niet meer gebruikt.

2 Waarom?

Het begint allemaal met inzicht: als je weet wat je moet beschermen, kun je ook bepalen wat de moeite waard is om te verdedigen.

Niet alles hoeft beschermd te worden; je kunt er bewust voor kiezen om bepaalde zaken niet te verdedigen, zolang je die keuze maar weloverwogen maakt.

3 Hoe?

Kleinere organisaties kunnen dit handmatig aanpakken. Gebruik een spreadsheet en noteer welke toestellen je hebt en welke software daarop staat. Zorg ervoor dat je ook aangeeft wat cruciaal is voor je bedrijf en wat minder belangrijk is.

Grotere ondernemingen kunnen deze inventarisatie laten uitvoeren met een geautomatiseerde scan, eenmalig of periodiek, om altijd up-to-date te blijven.

Meer info

Een doeltreffende cybersecurity start met een overzicht van alle hardware en software binnen je bedrijf.

Module Id - Hoe begin je eraan

www.unizo.be/cs4zo

2. Update

Het updaten van software is essentieel voor de veiligheid en prestaties van je systemen. Updates verhelpen kwetsbaarheden en voorkomen dat hackers deze misbruiken. Ze zorgen ook voor betere functionaliteit en stabiliteit. Door regelmatig te updaten, bescherm je je systemen tegen bedreigingen en houd je je software optimaal werkend.

1 Wat?

Zorg ervoor dat je security updates zo snel mogelijk uitvoert, bij voorkeur automatisch. Dit geldt niet alleen voor je besturingssystemen, zoals Windows, maar ook voor alle programma's en machines die je gebruikt, machines worden vaak over het hoofd gezien.

Controleer daarnaast of al je programma's nog te updaten zijn. Soms is de software te oud of kan je hardware de nieuwste versie niet aan.

2 Waarom?

Software wordt door mensen geschreven, en mensen maken fouten. Daardoor bevat software altijd fouten.

Security updates herstellen deze fouten. Als je die updates niet uitvoert, kunnen hackers deze kwetsbaarheden (bugs) misbruiken om controle te krijgen over jouw apparaten.

3 Hoe?

Kleinere organisaties kunnen dit handmatig doen. Gebruik de inventaris uit punt 1 en controleer wekelijks of tweewekelijks al je software om updates uit te voeren.

Grotere bedrijven zouden dit proces moeten automatiseren en regelmatige scans uitvoeren om zeker te zijn dat alle software up-to-date is.

Meer info

Regelmatige updates beschermen je systemen tegen kwetsbaarheden en zorgen voor optimale veiligheid.

Module 4a- Malware
Module 4b - Ransomware

www.unizo.be/cs4zo

3. Multi-factor

Multi-factor authenticatie (MFA) biedt een essentiële extra beveiligingslaag door naast een wachtwoord een tweede vorm van identificatie te vereisen, zoals een sms-code of biometrische scan. Dit maakt het voor onbevoegden veel moeilijker om toegang te krijgen, zelfs bij een gestolen wachtwoord. MFA versterkt de bescherming van je gevoelige informatie en is onmisbaar in de strijd tegen geavanceerde cyberdreigingen.

1 Wat?

Multi-factor authenticatie (MFA) voegt een extra beveiligingslaag toe bovenop je wachtwoord. Dit kan een SMS-code of een code in je authenticator-app zijn.

Je kunt MFA instellen voor het opstarten van je pc en voor toegang tot je meest kritische applicaties zoals je mailbox, administratie of machineconfiguratie.

2 Waarom?

Een wachtwoord alleen is tegenwoordig niet meer voldoende. Hoewel een sterk wachtwoord essentieel is, kunnen hackers het alsnog stelen, raden of kraken.

Met een tweede factor moeten ze niet alleen het wachtwoord achterhalen, maar ook toegang krijgen tot je tweede beveiligingssysteem, wat het voor hen veel te complex maakt.

3 Hoe?

Je kunt zelf kiezen welke vorm van multi-factor authenticatie je gebruikt. Authenticator-apps zijn veiliger dan SMS-codes. Biometrische beveiliging op je smartphone is meestal nog beter dan een authenticator-app. Zelfs de minst sterke optie, zoals een SMS-code, biedt echter een waardevolle extra beveiligingslaag bovenop je wachtwoord.

Zorg ervoor dat je dit toepast op alle belangrijke software in je onderneming en zeker bij het opstarten van je pc en het openen van je mailbox.

Meer info

Met MFA bescherm je je accounts beter, zelfs als je wachtwoord wordt buitgemaakt.

Module 3a - Paswoorden
Module 3b - MFA

www.unizo.be/cs4zo

Met de juiste partij in zee!

Een goede IT-partner is essentieel voor elk bedrijf. Technologie speelt een cruciale rol in dagelijkse operaties en strategische keuzes. Een betrouwbare IT-partner zorgt niet alleen voor een stabiele infrastructuur en dataveiligheid, maar helpt ook bij het volgen van technologische evoluties en het tijdig upgraden van systemen. Zo blijf je als bedrijf efficiënt, veilig én klaar voor groei.

Wat je zelf doet, doe je niet altijd beter!

Een goede IT-partner zorgt ervoor dat je bedrijf mee is met de nieuwste technologieën en best practices. Ze volgen de IT-markt nauwgezet, adviseren over relevante innovaties en helpen je om verouderde systemen tijdig te upgraden. Zo werk je steeds met betrouwbare en efficiënte oplossingen die je helpen om kosten te besparen, productiviteit te verhogen en je onderneming klaar te stomen voor groei.

Een sterke IT-partner zorgt voor een stabiele infrastructuur, optimale beveiliging en helpt je bedrijf mee te groeien. Ze bieden pro-actieve ondersteuning, volgen techno-logische evoluties op en adviseren strategisch, zodat jij efficiënter werkt en klaar bent voor de toekomst.

Bovendien bieden ze proactieve ondersteuning. In plaats van te wachten tot er iets misloopt, detecteren en verhelpen ze problemen op voorhand. Dit voorkomt stilstand en zorgt ervoor dat je bedrijfsprocessen vlot blijven draaien.

Cyberveiligheid is een ander speerpunt. IT-partners beschermen je systemen met up-to-date beveiligingsmaatregelen, voeren regelmatige controles uit en bieden trainingen aan voor medewerkers. Zo vergroot je de digitale weerbaarheid van je hele organisatie.

Tot slot zijn ze meer dan alleen technische hulp, een goede IT-partner is ook een strategische sparringpartner. Ze denken mee over de lange termijn en helpen je om technologie slim in te zetten in functie van je bedrijfsdoelen.

4. Isoleren

Isolatie voorkomt dat één zwak punt je hele netwerk in gevaar brengt. Koppel verouderde of slecht beveiligde systemen los, beperk hun internettoegang en houd ze weg van je dagelijkse werkomgeving. Zo bescherm je ook je cruciale systemen beter tegen hackers.

1 Wat?

Zorg dat je onderneming zoveel mogelijk uit gescheiden 'eilandjes' bestaat. Koppel PC's die niet per se in hetzelfde netwerk hoeven te zitten of via software die controle neemt over de machines, los.

Software of machines die je niet up-to-date kunt houden of niet kunt beveiligen met multifactor authenticatie, moeten ook losgekoppeld worden van de rest.

2 Waarom?

Een hacker zal altijd op zoek gaan naar de zwakste schakel en via die route proberen door te dringen tot de kritieke onderdelen van je onderneming. Soms heb je geen keuze en moet je oude machines behouden of kun je bepaalde software niet beveiligen met multi-factor authenticatie.

Dit zijn je zwakke schakels. Door deze onderdelen los te koppelen van de rest van je systeem, voorkom je dat ze de rest van je bedrijf kunnen 'besmetten'.

3 Hoe?

Start met een inventarisatie: welke software of hardware is moeilijk te beveiligen door bv. gebrek aan updates of MFA? Isoleer deze zwakke schakels en zorg dat ze niet bereikbaar zijn vanaf je gewone pc en beperk hun internettoegang.

Pas dit isolatieprincipe ook toe op je cruciale systemen, zoals machines, om ze extra te beschermen tegen hackers.

Meer info

Isolatie beperkt risico's door kwetsbare systemen los te koppelen van je netwerk?

Module 1b - Basis tips
Module 4c - Data theft

www.unizo.be/cs4zo

Ontdek de lespaketten

CS4ZO – CyberSecurity voor Zelfstandige Ondernemers is een initiatief van UNIZO dat zelfstandigen en kmo's helpt om zich beter te wapenen tegen cyberdreigingen. Het programma sluit aan bij de Belgische Cybersecurity Strategie en richt zich op een stapsgewijze aanpak, aangepast aan de noden van zowel kleine zelfstandigen als grotere kmo's.

Het programma biedt gratis videolessen, podcasts, microlearnings en handige gidsen over de belangrijkste thema's in cybersecurity.

De basis

- De KMO. Doelwit van hackers.
- Veilig omgaan met je PC.
- Veilig omgaan met je smartphone.
- Je zaak beschermen tegen hackers. Hoe begin je eraan?

Phishing

- Standaard phishing.
- Geavanceerd phishing.
- Hacking in de praktijk. Datadiefstal.

Paswoorden

- Paswoorden.
- Multi-factor authenticatie.
- Hacking in de praktijk.
- Factuurfraude.

Malware

- Malware.
- Ransomware.
- Datadiefstal.
- Hacking in de praktijk.
- Ransomware.

Alles rond je onderneming

- Aanvallen op de toeleveringsketen.
- Thuis - Werk.
- Wifi - Cloud - VPN.
- Mijn website.

Better safe than sorry

- Beveiligingsmonitoring.
- Maatregelen. Alles op een rij.
- Cyber Wargame.

Nelissen Steenfabrieken

Nelissen Steenfabrieken, opgericht in 1921, is een toonaangevende producent van handvormgevelstenen en steenstrips. Vanuit de groeve in Kesselt produceert het familiebedrijf jaarlijks meer dan 185 miljoen stenen, in meer dan honderd kleuren en formaten. Naast gevelstenen biedt Nelissen ook gevelisolatiesystemen, lijmen, voegmortels en snelbouwblokken aan. Met een sterke focus op innovatie en duurzaamheid groeide Nelissen uit tot een internationale referentie in gevelmaterialen, waar kwaliteit en esthetiek hand in hand gaan.

Wat betekent digitalisering binnen jullie bedrijf?

Frank Aussems, IT-manager bij Nelissen Steenfabrieken: Binnen onze digitale transformatie ligt de focus op het creëren van een digitale customer journey voor onze bezoekers, én op het automatiseren en optimaliseren van onze bedrijfsprocessen.

Wat is de belangrijkste reden om te digitaliseren?

Dankzij de automatisatie van onze bedrijfsprocessen kunnen we vandaag zowel strategisch als operationeel data-gedreven beslissingen nemen. Een bedrijf runnen op buikgevoel alleen volstaat simpelweg niet meer.

Dankzij de automatisatie van onze bedrijfsprocessen kunnen we vandaag zowel strategisch als operationeel data-gedreven beslissingen nemen. Een bedrijf runnen op buikgevoel alleen volstaat simpelweg niet meer.

Frank Aussems, **IT Manager Nelissen Steenfabrieken**

Is jullie onderneming reeds actief in de cloud?

Onze bedrijfskritieke toepassingen draaien momenteel nog on-premise, maar we evolueren stilaan naar een hybride structuur, omdat steeds meer applicaties ook in de cloud beschikbaar zijn.

Wat is de belangrijkste reden om te werken in de cloud?

Gegevens en applicaties zijn vandaag toegankelijk vanaf verschillende locaties en toestellen. Dat verhoogt de productiviteit en efficiëntie van onze medewerkers aanzienlijk.

Welke maatregelen hebben jullie al genomen rond cybersecurity?

Naast de traditionele maatregelen zoals firewalls, netwerksegmentering en back-ups, zetten we vandaag sterk in op monitoring en de bescherming van onze endpoints. Hiervoor werken we samen met Office-IT, onder andere met tools zoals NinjaOne en SentinelOne.

Zijn jullie medewerkers zich bewust van mogelijke cybersecurity risico's?

Op dit moment zetten we nog niet actief in op specifieke awareness-toepassingen om onze gebruikers te sensibiliseren rond phishing. De communicatie verloopt voorlopig vooral intern, maar dit is zeker een aspect dat we in de toekomst verder willen ontwikkelen.

AI, we kunnen er niet omheen! Hebben jullie hieromtrent al stoppen ondernemen?

Vandaag experimenteren we met AI, vooral binnen onze productieomgeving, waar we zoeken naar manieren om de kwaliteitscontrole verder te optimaliseren. Ook binnen onze customer journey zetten we in op digitale tools die klanten helpen bij het maken van de juiste keuze. Die tools stellen ons in staat om een visueel beeld te creëren van de steen zoals de klant die voor ogen heeft. Met de technologie hier aan tafel kunnen we dat al realiseren, en binnenkort kunnen we die ervaring nog versterken in onze Bricksperience-ruimte.

Zijn jullie als onderneming bewust van de mogelijke risico's van AI?

We zijn ons zeker bewust van de risico's rond AI, vooral wat betreft het onbedoeld blootstellen van bedrijfsdata op het internet.

Wat is de belangrijkste reden om AI te gebruiken binnen jullie onderneming?

We zien AI vooral als een middel om repetitieve taken te automatiseren, zodat onze medewerkers zich kunnen focussen op waardevollere taken.

Hoe zien jullie de toekomst van en de impact van digitalisering in de komende jaren?

We blijven volop inzetten op digitale technologieën om duurzamer te werken. Denk aan smart factoring, slim energiebeheer en het verminderen van afval via data-analyse. De focus ligt daarbij op maatschappelijk verantwoord ondernemen, waarbij we technologie inzetten om onze ESG-doelstellingen te realiseren.

Ga voor een strategische compagnon de route!

Wat is het belang van een IT-partner voor jullie onderneming?

Omdat we de specifieke kennis rond de opzet en configuratie van onze infrastructuur niet in huis hebben, vertrouwen we volledig op de expertise en ervaring van onze partner Office-IT. Zij zorgen voor de nodige ondersteuning en waarborgen de continuïteit van ons bedrijf.

Wat verwachten jullie van de IT-partner?

Het geeft ons gemoedsrust dat we op elk moment kunnen rekenen op de ondersteuning van Office-IT.

Neemt Office-IT een pro-actieve rol op en hoe vertaalt zicht dat?

Die proactieve rol komt vooral tot uiting via onze monitoringtool, waarmee Office-IT vandaag zelfs preventief kan ingrijpen nog vóór er zich problemen voordoen. Daarnaast plannen we jaarlijks een overleg met Office-IT om nieuwe ontwikkelingen te bespreken en te bekijken hoe die kunnen bijdragen aan de groei van onze organisatie.

Wat is de impact van de samenwerking met Office-IT?

De samenwerking met Office-IT ontzorgt ons op het vlak van IT-infrastructuur en brengt zo rust binnen onze organisatie.

Wie is Office-IT?

Joeri Vael, account Manager bij Office-IT: Office-IT is een managed service provider, wat betekent dat we via een uitgebreid monitoring-

Joeri Vael
Account manager Office-IT

systeem de volledige IT-infrastructuur van onze klanten opvolgen. We kunnen proactief ingrijpen en bieden zo maximale ontzorging.
Binnen Office-IT ben ik verantwoordelijk voor het account-management: alles wat de klant nodig heeft, regel ik. Daarnaast sta ik ook in voor zowel de verkoop als de aankoop.

Hoe is de samenwerking tussen Office-IT en Nelissen Steenfabrieken

Onze samenwerking met Nelissen Steenfabrieken gaat terug tot het midden van de jaren '90. Office-IT bestaat in zijn huidige vorm sinds 2012, maar het merendeel van ons team werkt al samen sinds eind jaren '90, dus eigenlijk vanaf het begin van onze samenwerking met Nelissen Steenfabrieken.

We nemen er het volledige IT-beheer op ons: van servers en infrastructuur tot de ondersteuning bij de aankoop van nieuwe werkstations en firewalls. Ook op vlak van cybersecurity zorgen we ervoor dat alles tiptop in orde is.

5. Bewustzijn

De mens is vaak de zwakste schakel in cybersecurity. Een ondoordachte klik of slordig wachtwoord kan volstaan om een hacker binnen te laten. Cybercriminelen mikken breed en hopen dat iemand ergens een fout maakt, en dat kan evengoed bij jou op kantoor zijn. Daarom is bewustmaking essentieel: leg in klare taal uit waar medewerkers op moeten letten én waarom. Alleen wie het belang begrijpt, is bereid om veilig te werken, ook als dat iets minder comfortabel is.

1 Wat?

De mens wordt vaak gezien als de zwakste schakel in cybersecurity. Door gebrek aan kennis over de impact van onze acties, maken we bijna dagelijks kleine foutjes die hackers gemakkelijk kunnen uitbuiten.

De grootste aandachtspunten zijn phishing, het veilig beheren van wachtwoorden, en het strikt gescheiden houden van privé- en werkgegevens in de digitale omgeving.

2 Waarom?

Hackers richten zich zelden op specifieke slachtoffers; ze zijn opportunisten. Ze sturen hun aanvallen als hagel de wereld in, zonder te letten op wie er geraakt wordt. Hun gedachte: iemand zal wel een fout maken en in de val trappen.

Als die persoon toevallig in jouw bedrijf werkt, kan hij of zij onbewust de deur voor hackers openzetten.

3 Hoe?

Leg medewerkers in eenvoudige taal uit waar ze op moeten letten en waarom dat belangrijk is.

Besteed voldoende aandacht aan het waarom. Veiliger werken op je pc gaat vaak ten koste van gebruiksvriendelijkheid. Mensen zijn alleen bereid dat 'offer' te brengen als ze begrijpen wat de meerwaarde is.

Meer info

Menselijke fouten blijven een groot cyberrisico, dus is bewustmaking cruciaal om veilig gedrag te stimuleren.

Module 2a - Phishing
Module 2b - Advanced phishing
Module 5b - Prive-werk

www.unizo.be/cs4zo

6. Anti-virus

Antivirussoftware is cruciaal voor de beveiliging van een bedrijf, omdat het beschermt tegen virussen, malware en andere cyberdreigingen die systemen kunnen verstoren en gegevens kunnen stelen. Het fungeert als een eerste verdedigingslinie door verdachte activiteiten te blokkeren en regelmatig te scannen. In een tijd van toenemende cyberaanvallen is het up-to-date houden van antivirussoftware een essentieel onderdeel van een sterke cybersecuritystrategie.

1 Wat?

Antivirussoftware is als basis-hygiëne voor je pc's en servers. Hoewel een antivirus alleen niet genoeg is, is een apparaat zonder antivirus een gemakkelijke prooi.

Zie antivirus als het slot op je voordeur: de eerste barrière waar een hacker omheen moet zien te komen.

2 Waarom?

Hackers proberen automatisch elk apparaat dat via het internet bereikbaar is te infecteren met malware.

Antivirusbedrijven volgen deze geautomatiseerde aanvallen continu en zorgen ervoor dat hun software deze bedreigingen blokkeert.

3 Hoe?

Het antivirussoftware pakket dat je kiest, maakt niet zoveel uit; de grote namen presteren vrijwel gelijk in vergelijkende studies. Het belangrijkste is dat je de software op alle pc's en servers installeert en deze up-to-date houdt om nieuwe bedreigingen effectief te detecteren. Idealiter combineer je antivirussoftware met een monitoringsdienst, zodat professionals de meldingen van de software evalueren en je waarschuwen als er meer aan de hand is.

Meer info

Antivirussoftware vormt een essentiële eerste verdedigingslinie tegen malware en cyberaanvallen.

Module 4a - Malware
Module 4b - Ransomware
Module 6a - Security Monitoring

www.unizo.be/cs4zo

Cybersecurity zonder paniek, mét plan

Bert Bleukx
Stark Security

Cybersecurity is een verhaal met vele facetten, en als ondernemer is het soms moeilijk om door de bomen het bos nog te zien. Cyberdreigingen evolueren razendsnel, in de media lezen we bijna dagelijks over nieuwe aanvallen, datalekken & miljoenenverliezen door ransomware.

De valkuil? Je laten leiden door angst of paniek. Misschien hoorde je van een getroffen concullega, of kreeg je een alarmerend bericht van een IT-leverancier. Maar angst is een slechte, en vaak dure, raadgever.
Wat je nodig hebt, is geen paniekreactie, maar een cybersecuritystrategie, een plan dat in kaart brengt waar je risico's liggen en welke stappen je in welke volgorde moet zetten. Cyberveiligheid is geen einddoel, maar een voortdurend proces van inschatten, aanpassen en versterken.

Een veelvoorkomende fout bij cybersecurity is dat ondernemers denken dat ze alles in één keer moeten oplossen. Maar net zoals je een bedrijf niet in één dag bouwt, bouw je ook cybersecurity stap voor stap.

Begin met het laaghangend fruit. Dit zijn maatregelen die weinig kosten en meteen impact hebben:

- Gebruik multi-factor authenticatie (MFA) op alle kritieke accounts.
- Houd software en systemen up-to-date om kwetsbaarheden te dichten.
- Zorg voor regelmatige back-ups en test of je ze vlot kunt herstellen.
- Train je medewerkers in het herkennen van phishing en andere dreigingen.
- Segmenteer je netwerk, zodat een aanval op één onderdeel niet meteen alles platlegt.

Een cybersecurityplan is echter nooit 'af'. Net zoals je bedrijfsstrategie verandert met de markt, moet je beveiliging regelmatig herbekeken en aangepast worden. Nieuwe dreigingen ontstaan, technologieën evolueren en hackers worden steeds geavanceerder. Daarom is bijsturing essentieel, een plan dat vijf jaar onaangeroerd blijft, biedt geen bescherming meer.

Een cybersecurityplan is echter nooit af. Net zoals je bedrijfsstrategie verandert met de markt, moet je beveiliging regelmatig herbekeken en aangepast worden.

De eerste stap? Informeren. Want je kunt pas actie ondernemen als je weet wat je moet doen. Deze gids is een goed begin, maar je kunt cybersecurity pas echt implementeren als je de juiste kennis hebt.

Cybersecurity is geen kwestie van 'of' maar 'wanneer' je ermee aan de slag gaat. Begin vandaag, stap voor stap, en maak je onderneming sterker.

7. Toegang op afstand

Toegang op afstand biedt medewerkers de flexibiliteit om vanop eender welke locatie te werken, maar brengt ook extra cyberrisico's met zich mee. Zonder de juiste beveiligingsmaatregelen kunnen onbevoegden via die weg toegang krijgen tot gevoelige bedrijfsgegevens. Daarom is het essentieel om toegang op afstand altijd te beveiligen met sterke wachtwoorden, multi-factor authenticatie en een beveiligde verbinding, zoals een VPN. Ook regelmatige monitoring en toegangscontroles zijn cruciaal.

1 Wat?

Wanneer je vanuit huis werkt of wanneer gespecialiseerde firma's op afstand verbinding maken met jouw systemen, gebeurt dat meestal via een VPN.

Zo'n VPN moet veilig worden opgezet, omdat het een directe toegangsdeur tot je bedrijf vormt.

2 Waarom?

Alles wat aan het internet hangt, wordt gevonden door hackers. Als daar een zwakke plek in gevonden wordt, wordt dit misbruikt om binnen te breken.

Een VPN hangt per definitie aan het internet. Hackers weten maar al te goed hoe veelvuldig deze technologie gebruikt wordt én hoe vaak ze onzorgvuldig wordt geconfigureerd of onderhouden.

3 Hoe?

Zorg altijd voor multi-factor authenticatie bij je VPN-verbindingen, zowel voor jou en je medewerkers bij thuiswerken als voor partners die onderhoud aan je systemen uitvoeren. Schakel VPN-verbindingen uit wanneer je ze niet nodig hebt. Als een bedrijf bijvoorbeeld één dag per maand onderhoud doet, zorg dan dat hackers de verbinding de overige 30 dagen niet kunnen misbruiken.

Houd je VPN-software altijd up-to-date; security updates zijn essentieel, vooral voor toegangspunten tot je bedrijf.

Meer info

Toegang op afstand biedt flexibiliteit, maar vraagt om sterke beveiliging om misbruik en datalekken te voorkomen.

Module 1b Basic tips & tricks
Module 3b MFA
Module 5c Wifi-VPN-Cloud

www.unizo.be/cs4zo

Dustin Benner
ClearMedia

Expert aan het woord

Als zelfstandige of kleine ondernemer ben je voortdurend bezig met je klanten, je dienstverlening en het draaiende houden van je zaak. Cybersecurity staat dan vaak niet bovenaan je prioriteitenlijst. Toch wordt élke ondernemer, groot of klein, steeds afhankelijker van digitale technologieën en online systemen. En daarmee groeit ook het risico op cyberaanvallen.

In tegenstelling tot grote bedrijven met een gespecialiseerde IT-afdeling, sta je als zelfstandige, micro- of kleine onderneming vaak alleen voor de beveiliging van je bedrijf. Hackers weten dat en richten zich bewust op dat type van ondernemingen, omdat die meestal minder beveiligingsmaatregelen hebben. Een cyberaanval kan niet alleen leiden tot verlies van waardevolle gegevens, maar ook je bedrijfsvoering stilleggen. Zonder toegang tot je klantengegevens, facturatie of boekhoudsoftware sta je met de rug tegen de muur.

Cyberveiligheid, ook voor zelfstandigen en kleine bedrijven onmisbaar.

De grootste cyberrisico's voor kleine ondernemingen

Je hoeft geen IT-expert te zijn om je risico's te begrijpen. De meest voorkomende dreigingen zijn:

- **Phishing**: Valse e-mails die je proberen te misleiden om op een link te klikken of inloggegevens door te geven.
- **Ransomware**: Kwaadaardige software die je bestanden versleutelt en pas vrijgeeft na betaling van losgeld.
- **Datalekken**: Het verlies van klanten-gegevens door een hack of menselijke fout kan juridische en financiële gevolgen hebben.

Wat kun je zelf doen?

Cyberveiligheid hoeft niet complex of duur te zijn. Een paar eenvoudige maatregelen maken al een wereld van verschil:

- Gebruik sterke wachtwoorden en activeer multi-factor authenticatie (MFA) op je e-mails en bedrijfssoftware.
- Werk je software en toestellen regelmatig bij zodat beveiligingslekken gedicht worden.
- Wees alert op verdachte e-mails en train jezelf en eventuele medewerkers in het herkennen van cyberdreigingen.
- Maak back-ups van je belangrijkste gegevens en bewaar die op een aparte locatie.
- Gebruik een betrouwbare antivirus- en firewalloplossing om malware te blokkeren.

Meer dan technologie: bewustwording en wetgeving

Cybersecurity draait niet alleen om technologie. Het gaat ook om bewuste keuzes maken en veilig online gedrag. Als zelfstandige ben jij zélf de eerste verdedigingslinie. Dat betekent bijvoorbeeld dat je niet zomaar software moet installeren van onbekende bronnen of je bedrijfswachtwoorden niet op een post-it naast je computer moet bewaren.
Daarnaast verplicht de wetgeving je om zorgvuldig met persoonsgegevens om te gaan. De Algemene Verordening Gegevensbescherming (AVG) eist dat je klantengegevens correct bewaart en beveiligt.

Begin vandaag, stap voor stap

Je hoeft niet alles tegelijk te doen. Start met kleine, haalbare stappen die direct effect hebben. Door bewust met cybersecurity om te gaan, bescherm je niet alleen je onderneming, maar ook je klanten en leveranciers.

Wil je meer weten?

Bekijk dan de UNIZO-videolessen over cybersecurity en ontdek hoe je je zaak beter kunt beveiligen zonder onnodige kosten of complexe IT-oplossingen.

8. Wargame

Een wargame of simulatie is een onmisbaar onderdeel van een doordachte cybersecuritystrategie. Door een denkbeeldige cyberaanval stap voor stap te doorlopen, ontdek je waar de zwakke plekken zitten in je organisatie en hoe goed je team is voorbereid op een echte crisissituatie. Zo'n oefening maakt risico's tastbaar, verhoogt het bewustzijn bij medewerkers en helpt je om sneller, gerichter en doeltreffender te reageren als het écht misgaat.

1 Wat?

Zie het als een brandoefening, maar dan voor je digitale wereld. Wat als... Simuleer een hacking-aanval op papier en beoordeel hoe goed je bent voorbereid om zo'n aanval te weerstaan.

Ga ervan uit dat het al gebeurd is, wat doe je dan?

2 Waarom?

Als je slachtoffer wordt van een hack, is paniek een slechte raadgever. Door van tevoren te oefenen op zulke situaties, kun je veel beter en effectiever beslissingen nemen.

Goede communicatie is cruciaal tijdens een aanval; door hier vooraf over na te denken, zorg je ervoor dat je communicatie veel beter verloopt dan wanneer je het op het moment zelf moet improviseren.

3 Hoe?

Overleg met belangrijke personen over mogelijke aanvallen: wat zou echt schadelijk zijn als het gebeurt? Simuleer vervolgens een scenario waarin dit al is gebeurd en bedenk acties om de schade te beperken. Je hebt ICT nodig om alles te herstellen, maar dat kost tijd.

De vraag is: hoe overbrug je die tijd? Wat vertel je aan klanten en leveranciers, en hoe kun je ondanks de hack je bedrijfsactiviteiten voortzetten?

Meer info

Een simulatie van een cyberaanval helpt je inschatten hoe goed je bent voorbereid op een echte digitale crisis.

Module 4a - Malware
Module 4b - Ransomware
Module 6a - Security Monitoring

www.unizo.be/cs4zo

Cyberverzekering: is het nodig voor jouw onderneming?

Cybercriminaliteit stopt niet bij grote bedrijven. Ook zelfstandigen en kleine ondernemingen zijn een doelwit, vaak omdat hun beveiliging minder sterk is. Een cyberaanval kan ernstige gevolgen hebben: van gestolen klantengegevens tot een vergrendeld facturatie-systeem waardoor je je werk niet meer kunt doen. Een cyberverzekering kan helpen om de financiële schade te beperken, maar is het ook een slimme investering voor jouw onderneming?

Waarom zou je een cyberverzekering overwegen?

Je auto, brandverzekering en beroeps-aansprakelijkheid heb je waarschijnlijk goed geregeld. Maar als je bedrijf afhankelijk is van digitale systemen, en dat is bij de meeste ondernemers het geval, is de vraag: wat gebeurt er als een cyberaanval je bedrijf platlegt?

Een cyberverzekering helpt je om:

- De kosten van een cyberaanval op te vangen : Denk aan IT-forensisch onderzoek, herstel van systemen en juridische bijstand.
- Je bedrijf draaiende te houden: Als je bedrijf tijdelijk offline moet, kan een verzekering inkomstenverlies (gedeeltelijk) dekken.
- Schadeclaims door klanten te vermijden: Als klantengegevens uitlekken, kan een verzekering helpen bij schadevergoeding en juridische kosten.
- Hulp te krijgen van specialisten: Veel verzekeraars bieden crisismanagement aan, zodat je snel de juiste experts inschakelt.

Wat dekt een cyberverzekering?

Niet elke cyberverzekering is hetzelfde, maar in de meeste gevallen bieden ze dekking voor:

- **Herstelkosten**: IT-experts die systemen herstellen en data terughalen.
- **Bedrijfsschade**: Inkomstenverlies door downtime na een aanval.
- **Wettelijke kosten**: Boetes en claims bij datalekken of overtreding van de AVG.
- **Onderhandeling bij ransomware**: Begeleiding en hulp bij afpersing na een aanval.

Let op: sommige basispolissen dekken enkel IT-herstel, terwijl uitgebreidere polissen ook reputatieschade en juridische kosten vergoeden.

Hoe kies je de juiste cyberverzekering?

- **Evalueer je risico's**: Hoe afhankelijk ben je van digitale systemen? Heb je klantengegevens in beheer? Een webshop? Cloudsoftware?
- **Vergelijk polissen**: Niet elke verzekering dekt ransomware of datalekken op dezelfde manier. Kijk naar de kleine lettertjes.
- **Let op de voorwaarden**: Sommige verzekeringen eisen dat je basismaatregelen neemt, zoals een firewall en back-ups.
- **Kijk of je al verzekerd bent:** Soms biedt je bestaande verzekering al een basis cyberdekking.

NIS2-richtlijn, wat betekent dit voor mijn onderneming?

Misschien heb je al gehoord van de NIS2-richtlijn, een nieuwe Europese wetgeving die bedrijven verplicht om striktere cybersecurity-maatregelen te nemen.
Voor veel zelfstandigen en kleine ondernemingen is NIS2 niet direct van toepassing, maar de impact op je keten en klanten is wél belangrijk.
De nieuwe regels richten zich op bedrijven die als kritiek of essentieel worden beschouwd voor de economie, zoals telecom, energie, transport, financiële instellingen en leveranciers van digitale diensten. Zij moeten hun cyberbeveiliging aanzienlijk versterken en rapporteren over incidenten.

Maar wat betekent dat voor jou als kleinere onderneming?

Waarom NIS2 ook voor jou relevant is

- Jouw klanten en partners kunnen jou als zwakke schakel zien. Grotere bedrijven zullen striktere cybersecurity-eisen stellen aan hun leveranciers en dienstverleners, inclusief KMO's en zelfstandigen.
- Sterkere cybersecurity wordt een vereiste om mee te blijven spelen. Wil je blijven samenwerken met grotere klanten of overheden? Dan moet je misschien aantonen dat je basisbeveiliging op orde is.
- Een cyberaanval bij jou kan je hele supply chain raken. Zelfs als jij geen verplichtingen hebt onder NIS2, kan een hack in jouw onderneming gevolgen hebben voor andere bedrijven waarmee je samenwerkt.

Wat kun je doen?

Je hoeft niet meteen een volledig NIS2-compliant bedrijf te worden, maar je kunt wel zorgen dat je onderneming niet de zwakste schakel wordt.

Begin met:

- Sterke wachtwoorden en multi-factor authenticatie instellen op je belangrijkste accounts.
- Software up-to-date houden om beveiligingslekken te dichten.
- Back-ups maken en ze offline bewaren, zodat je snel kunt herstellen bij een aanval.
- Veilig omgaan met klantgegevens, want ook de AVG (GDPR) stelt hier regels voor.
- Je bewust worden van phishing en social engineering-aanvallen, zodat je niet per ongeluk de deur openzet voor cybercriminelen.

Cybersecurity wordt een concurrentievoordeel. Bedrijven die hun basisbeveiliging op orde hebben, kunnen aantonen dat ze een betrouwbare partner zijn.

Wil je weten of NIS2 voor jouw sector verplicht is? Bezoek de website van Safe-on-web@work en check de Belgische regels.

Safeonweb@work

Safeonweb@work is een initiatief van het Centrum voor Cybersecurity België (CCB) voor Belgische organisaties en ondernemingen. Het doel is de cyberveiligheid van de Belgische ondernemingen en organisaties te versterken door hen via verschillende diensten advies, aanbevelingen en instrumenten te verstrekken waarmee ze de kwetsbaarheden van hun systemen kunnen identificeren en verzachten en worden gewaarschuwd over cyberbedreigingen.

7 stappenplan

Maak jouw organisatie klaar voor de NIS2-richtlijn met onze zeven cruciale stappen. Van het in kaart brengen van kwetsbaarheden tot het opleiden van je medewerkers, deze praktische stappen helpen je om je IT-beveiliging te versterken en aan alle vereisten te voldoen.

1. Heeft NIS2 op mij betrekking?
2. Registreer jouw NIS2-entiteit zo snel mogelijk
3. Meld significante incidenten
4. Voer een strategische risicobeoordeling uit
5. Plan cyberbeveiligings-training
6. De beveiligings-maatregelen implementeren
7. De beveiligingsmaat-regelen controleren

Wil je meer weten?

Raadpleeg de aanbeveling van het Centrum voor Cybersecurity België (CCB) om in 7 stappen te voldoen aan de Belgische NIS2-wetgeving.

Safeonweb.be @work

Conclusie

De bouwsector draait allang niet meer enkel om stenen en staal, maar ook om digitale connectiviteit. In een wereld van BIM-modellen, cloudgebaseerde projectplanning en samenwerkingen tussen tal van onderaannemers is IT niet langer ondersteunend, maar fundamenteel. Die digitale versnelling biedt enorme kansen voor efficiënter bouwen en beter samenwerken, maar verhoogt tegelijk ook de kwetsbaarheid.

Cybersecurity als bouwproject, geen eindpunt

Cyberveiligheid hoeft geen ingewikkeld verhaal te zijn. De gids reikt duidelijke bouwstenen aan die elk bedrijf kan toepassen: van het inventariseren van je systemen en het updaten van software, tot het implementeren van multi-factor authenticatie, netwerkisolatie en gebruikersbewustzijn. Ook tools zoals antivirussoftware, Mobile Device Management en een incident responseplan dragen bij aan een solide digitale basis.

NIS2 en ketenverantwoordelijkheid

Met de komst van de Europese NIS2-richtlijn wordt ook voor de bouwsector duidelijk dat cybersecurity niet langer vrijblijvend is. Zelfs als jouw onderneming niet rechtstreeks onder de wet valt, zullen grotere klanten en partners strengere eisen stellen aan leveranciers. Cyberveiligheid wordt daarmee niet alleen een noodzaak, maar ook een concurrentievoordeel. Bedrijven die kunnen aantonen dat hun basisbeveiliging op orde is, versterken hun positie in de keten.

Cyberverzekering als vangnet

Een cyberverzekering kan geen incidenten voorkomen, maar wel helpen om de schade te beperken. Van IT-forensisch onderzoek en juridische ondersteuning tot inkomensverlies en reputatieschade: wie voorbereid wil zijn op het ergste, doet er goed aan om ook dit aspect mee te nemen in zijn digitale strategie. De gids legt uit waarop je moet letten bij het kiezen van de juiste polis.

De rol van de IT-partner

Geen enkel bedrijf hoeft deze weg alleen te bewandelen. Een goede IT-partner is meer dan technische ondersteuning, het is een strategische meedenker. Of het nu gaat om cloudmigraties, cybersecuritymaatregelen of proactieve monitoring: wie kiest voor de juiste partner, bouwt aan continuïteit, efficiëntie en gemoedsrust.

Actie, stap voor stap

Digitale weerbaarheid hoeft niet in één dag opgebouwd te worden. Begin met de laagdrempelige maatregelen, zoals wachtwoord-beheer of software-updates. Breid stap voor stap uit met gebruikersopleidingen, simulatieoefeningen (wargames) en ketenafspraken. Gebruik deze gids als een praktisch kompas, niet als een theoretisch rapport.

Cyberveiligheid is geen doel op zich, maar een voorwaarde om te blijven groeien, samenwerken en leveren in een digitale economie. Zet vandaag de eerste stap, zodat je morgen met vertrouwen kan blijven ondernemen.

Heb je vragen of nood aan ondersteuning bij de eerste stappen?

unizo

Contacteer de UNIZO Ondernemerslijn voor advies op maat van jouw onderneming of bezoek **www.unizo.be/cybersecurity** voor meer tools, tips en opleidingen.

+32 2 212 26 78

ondernemerslijn@unizo.be

Funded by
the European Union
NextGenerationEU