Zero trust, de nieuwe norm in cybersecurityland uitgelegd

inetum realdolmen
Positive digital flow

De wereld verandert. Uw security ook?

Er was een tijd dat een sterk wachtwoord, antivirussoftware en een firewall met VPN volstonden om uw organisatie te beschermen tegen cyberaanvallen. Helaas ligt die tijd lang achter ons.

Vandaag zijn we niet langer aan één vaste werkplek gebonden. En al evenmin aan één vast toestel. We werken mobiel, op verschillende devices, zelfs op eigen privétoestellen, en steeds vaker ook in de cloud.

Met die **groeiende complexiteit** van onze werkomgeving zijn ook de cyberrisico's en -gevaren gevoelig toegenomen. Eén enkel vast doelwit is nu eenmaal makkelijker te beveiligen dan vele bewegende doelwitten.

Dat we onze beveiligingsmiddelen moeten afstemmen op die nieuwe realiteit op de werkvloer, ligt voor de hand. Alleen zal een uitbreiding van ons beveiligingsarsenaal op zich niet volstaan: we hebben een wezenlijk andere kijk op security nodig om tot een volledig nieuwe aanpak te komen. Die **security shift** vergt bovendien een omslag in de cultuur van onze organisatie en de mindset van onze medewerkers.

"In 2022 zijn de cyberaanvallen opnieuw met **32 %** gestegen. Bijna 1 op 8 van de Vlaamse bedrijven werd het afgelopen jaar slachtoffer van een cyberaanval."

Zero trust security: nieuwe beveiligingsprincipes voor een nieuwe realiteit

Zero trust security. Kortweg: zero trust. Misschien had u er al van gehoord? Onder die noemer gaat een nieuwe, **proactieve benadering** van security schuil die u toelaat om sneller en efficiënter te reageren op bedreigingen en aanvallen effectief af te slaan en zelfs te voorkomen.

Daarvoor steunt zero trust op een brede waaier aan **adaptieve controlemiddelen en -mechanismen** en een proces van **continue verificatie**. Het volstaat bijgevolg niet om één enkel product, dienst, oplossing of technologie in huis te halen. Net zo min als u er zich met één enkel project of implementatie eens en voor altijd van af kan maken. Zero trust vergt een volgehouden inspanning op lange termijn en een voortdurende alertheid voor nieuwe risico's en gevaren.

AAN HET CONCEPT VAN ZERO TRUST LIGGEN DRIE BELANGRIJKE BASISPRINCIPES TEN GRONDSLAG:

1. **Verifieer uitvoerig en grondig:**
   Het belangrijkste principe achter het zero trust-beveiligingsmodel is "nooit vertrouwen, altijd verifiëren". Dat betekent bijvoorbeeld dat u toestellen standaard niet mag vertrouwen, zelfs als ze verbonden zijn met een geautoriseerd netwerk en zelfs als u ze eerder al eens heeft geverifieerd.

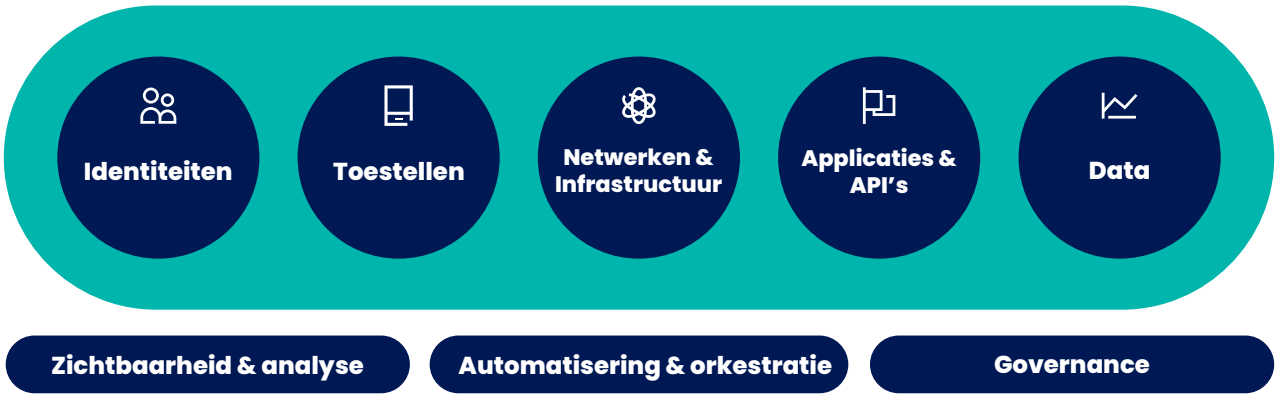
2. **Verleen toegang door zo weinig mogelijk privileges te geven:**
   Het principe van least privileged access (LPA) houdt in dat u de toegang tot uw werkomgeving tot het minimum beperkt (JEA, Just Enough Access) én dat u die toegang enkel verschaft op het moment en voor de tijd dat het nodig is (JIT, Just In Time).

3. **Ga ervan uit dat er inbreuken plaatsvinden:**
   Creëer uit voorzorg een infrastructuur die zo is ontworpen dat ze de impact van een inbreuk maximaal weet te beperken.

De architectuur achter zero trust security berust op vijf essentiële pijlers

WE ZETTEN ZE HIER KORT EVEN VOOR U OP EEN RIJTJE:

Basisprincipes van zero trust



Pijler 1: beveilig uw IDENTITEITEN

Alles begint met de gebruiker. Die kan over één of meer identiteiten beschikken. Aan elke identiteit zijn een aantal concrete gebruiksrechten en soms ook beheersrechten verbonden. Daarom is het van het allergrootste belang dat u die identiteit telkens grondig verifieert en de gebruiker steeds authenticeert voor u hem of haar toegang verleent tot uw werkomgeving (Identity & Access Management, IAM).

Een wachtwoord alleen, hoe sterk ook, volstaat daarvoor niet langer. Als we vandaag over **sterke authenticatie** spreken, dan hebben we het in de regel over **meervoudige authenticatie of MFA (Multi-Factor Authentication)**. Daarmee voegt u nog een extra beveiligingslaag toe aan uw toegangscontrole.

Belangrijk is niet alleen dat de verstrekte toegang "compliant" is – begrijp: in lijn met uw regels voor toegangscontrole – maar ook dat de toegang **typisch** is voor de identiteit die u verifieert.

Als een gebruiker probeert in te loggen vanuit India, terwijl hij zich fysiek in België bevindt, dan klopt er waarschijnlijk iets niet. In dat verband is het ook goed dat u die authenticatie nu kan baseren op een **risicoanalyse** die, naast de gebruiker en zijn toestel, ook de locatie en het gedrag van de gebruiker in rekening brengt.

Terwijl het gebruik van **single sign-on (SSO)** garandeert dat een gebruiker slechts eenmaal hoeft in te loggen om toegang te krijgen tot uw werkomgeving, zorgt het principe van **least privileged access (LPA)** ervoor dat diezelfde gebruiker niet zomaar overal toegang toe krijgt.

FOCUS OP MULTI-FACTOR AUTHENTICATION, SINGLE SIGN-ON, IDENTITY & ACCESS MANAGEMENT, PRIVILEGED IDENTITY MANAGEMENT AND RISK-BASED AUTHENTICATION

Pijler 2: beveilig uw TOESTELLEN

Eenmaal de authenticatie van de gebruiker goed en wel achter de rug is en zijn identiteit voldoende geverifieerd, krijgt hij toegang tot de resources in uw werkomgeving, waaronder ook uw data. Om die data op te vragen, maakt hij doorgaans gebruik van een "endpoint" of gebruikerstoestel zoals een pc of smartphone. Op die manier ontstaat er een **nieuw aanvalsoppervlak** dat we uiteraard ook opnieuw moeten bewaken en beschermen.

Om te beginnen gaan we regels opleggen om te verhinderen dat een onveilig toestel ooit toegang kan krijgen tot onze werkomgeving (**device compliance**). Zo kan u afdwingen dat een toestel door uw organisatie aangekocht en/of beheerd moet zijn om überhaupt voor zo'n toegang in aanmerking te komen. Ook kan u eisen dat het toestel voorzien is van een antivirusprogramma dat continu het gedrag en de conditie ervan monitort en de beveiliging automatisch op peil houdt (**endpoint protection**).

Eigenlijk komt het erop neer dat u de toestellen van uw gebruikers actief gaat beheren, ook wat het beveiligingsaspect betreft (**mobile device management, MDM**). Dat is des te meer een noodzaak geworden doordat gebruikers steeds vaker hun eigen privétoestellen meebrengen naar het werk (**bring your own device, BYOD**). Bovendien draaien op die toestellen vaak ook bedrijfsapplicaties zoals e-mail. Om de veiligheidsrisico's te beperken, moet u die toestellen dus wel mee gaan beheren. Dat beheer kan onder meer ook de mogelijkheid bevatten om data op afstand te wissen bij verlies van het toestel (**data loss prevention, DLP**).

"Naast het bedrijfsnetwerk is nu ook het thuisnetwerk van de gebruiker meer en meer een doelwit. Een makkelijke manier om veel mensen tegelijk te bereiken is de smartphone."

FOCUS OP MOBILE DEVICE MANAGEMENT, DEVICE COMPLIANCE EN ENDPOINT PROTECTION

Pijler 3: beveilig uw NETWERKEN en INFRASTRUCTUUR

Eenmaal voorbij de toegangscontrole, bevindt de gebruiker zich op uw netwerk. Via die infrastructuur krijgt hij uiteindelijk ook toegang tot de gegevens op de servers, databases en opslagsystemen in uw datacenter.

Om dat immense potentiële aanvalsoppervlak te verkleinen, is het belangrijk dat u uw netwerk in kleinere eenheden opdeelt of **segmenteert**. Dat deed u misschien eerder al door bijvoorbeeld via VLAN-technologie een virtuele scheiding aan te brengen tussen de clients en de servers op uw netwerk. Alleen volstaat dat niet langer. Voortaan is **microsegmentatie** aangewezen, op het niveau van de individuele apparatuur of zelfs de onderdelen daarvan, zoals een netwerkpoort. Door uw infrastructuur in nog kleinere en beter beschermde zones te verdelen, vermijdt u dat een virus bijvoorbeeld grote delen van uw infrastructuur diepgaand infecteert en lamlegt.

Daarnaast is het belangrijk dat u investeert in middelen om uw infrastructuur in reële tijd te monitoren en te beschermen tegen bedreigingen (**realtime threat protection**). Met een firewall kan u bijvoorbeeld verdacht netwerkverkeer op het spoor komen. Afwijkend, risicovol gedrag kan u automatisch laten markeren en signaleren, waarna u het kan blokkeren of andere beschermende maatregelen nemen.

Last but not least kan u ook uw netwerkverkeer zelf versleutelen (**end-to-end encryption**), om te vermijden dat het gecapteerd of gecompromitteerd wordt.

FOCUS OP SEGMENTATION, THREAT PROTECTION AND ENCRYPTION

Pijler 4: beveilig uw APPLICATIES & API'S

Applicaties en API's bieden de interface waarmee een gebruiker uw data kan raadplegen en benutten. Daarom is het belangrijk dat u het gebruik van die applicaties en API's zo goed mogelijk onder controle krijgt.

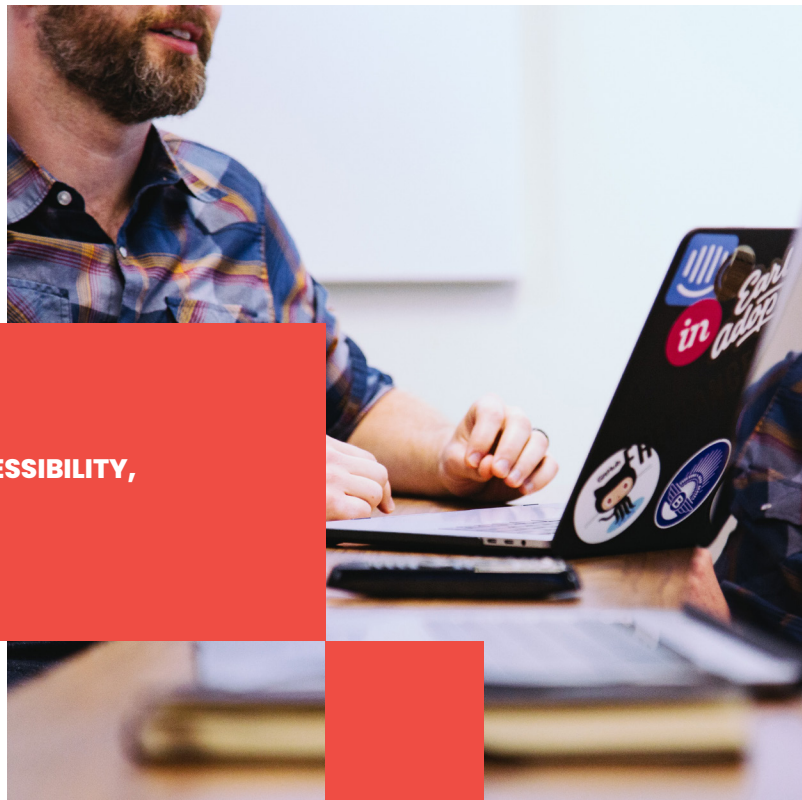
Een eerste belangrijke security-uitdaging voor IT-beheerders, als het op applicaties aankomt, is het fenomeen **shadow IT**: oplossingen die uw medewerkers buiten het gezichtsveld van uw IT-organisatie aanschaffen en aanwenden. Geen zicht hebben op die verraderlijke oplossingen in de schaduw van uw reguliere IT-omgeving vormt een heel groot risico. Investeer daarom in middelen waarmee u duidelijk in kaart kan brengen welke **niet-geautoriseerde applicaties** er allemaal binnen uw organisatie in gebruik zijn.

Besef echter dat ook **geautoriseerde applicaties** een beveiligingsrisico kunnen inhouden. Het is niet omdat het gebruik van een applicatie aanvaard en toegelaten is binnen uw organisatie, dat iedere medewerker er zomaar mee aan de slag kan en mag. Medewerkers moeten met name gemachtigd zijn om financiële of andere gevoelige informatie in een applicatie te consulteren (**in-app permissions**). Ook voor het toekennen en beheren van die machtigingen bestaan er intussen de nodige oplossingen.

Bovendien geldt ook hier dat u uw applicaties moet **screenen op afwijkend gedrag**. Dankzij het groeiende gebruik van API's kunnen applicaties tegenwoordig van overal data halen en met zo goed als alles communiceren. De keerzijde van die medaille is dat applicaties meer dan ooit blootgesteld zijn aan risico's en gevaren. Daarom kan u ook maar beter een strenge **toegangscontrole** instellen en handhaven, zeker voor uw kritieke applicaties.

Tot slot is het belangrijk om juist en op tijd te **patchen** om vulnerabilities in een software te dichten. Hoe langer u wacht met het installeren van de vereiste patch, hoe groter de kans op een cyberincident. Niet voor niets zijn de kwetsbaarheden of fouten in een programma vandaag een van de belangrijkste oorzaken van inbreuken. Vandaar het belang om op elk moment zicht te hebben op uw software vulnerabilities.

FOCUS OP ACCESS AUTHORIZATION, ACCESSIBILITY, MONITORING, PATCH MANAGEMENT



Pijler 5: beveilig uw DATA

Dit is waar het uiteindelijk allemaal om draait: het beveiligen van uw data. De vier voorgaande pijlers ondersteunen mee dat ultieme doel. Zonder die ondersteunende pijlers zou uw data lang niet zo veilig zijn. Dat neemt niet weg dat u er alle belang bij heeft om ook die data zelf zo goed mogelijk te beschermen. Zo zorgt u ervoor dat ze op elk moment veilig is, zelfs als ze – via e-mail of filesharing bijvoorbeeld – de applicaties, toestellen, infrastructuur en netwerken verlaat die u zelf zo zorgvuldig beheert.

Een eerste stap in dat beveiligingsproces is het **classificeren en labelen** van uw data. Zo kan u uw publieke data, waartoe iedereen toegang mag krijgen, scheiden van uw private of geheime data, die u in geen geval met de buitenwereld wenst te delen - en misschien zelfs niet met iedereen binnen uw organisatie.

"**23,5 %** van de geïmpacteerde bedrijven kreeg te maken met vernietiging van bedrijfsgegevens. **13,3%** werd getroffen door diefstal van bedrijfsgegevens."

Op basis van die classificatie en labeling kan u vervolgens ook voor uw data een zekere **toegangscontrole** instellen en handhaven. Door daarbij opnieuw het principe van **least priviliged access (LPA)** te hanteren, geeft u iedere gebruiker enkel toegang tot data die nodig is om zijn of haar functie naar behoren uit te oefenen – en niets meer dan dat.
Daarnaast beschikt u misschien over gevoelige, persoonsgebonden data, zoals medische gegevens. Daar moet u volgens de Europese GDPR-wetgeving heel zorgvuldig mee omgaan. Dat impliceert dat u die data moet **anonimiseren** of **pseudonimiseren**, als u ze toch wenst te gebruiken, bijvoorbeeld bij toepassingen voor big data.

We hadden het er ten slotte al eerder over: **encryptie**. Door uw kritieke data te versleutelen, vermijdt u dat die bij verlies of diefstal gelezen wordt. Oplossingen voor **data loss prevention (DLP)** stellen u bovendien in staat om achteraf, na het verlies of de diefstal, in te grijpen op uw data en die bijvoorbeeld te wissen. En als alles toch verkeerd zou gaan, is het goed om als laatste redmiddel op een **back-up** of kopie van uw data te kunnen terugvallen.

FOCUS OP CLASSIFICATION, LABELLING, ENCRYPTION, ACCESS AND DATA LOSS PREVENTION, BACKUP & RECOVERY

Extra fundamenten

De vijf geschetste pijlers die het bouwwerk van zero trust security meer dan stevig stutten, rusten op hun beurt op drie belangrijke steunlagen. Zij garanderen u een extra stevig fundament. Daarom loont het de moeite om ook in die onderbouw te investeren.

ZICHTBAARHEID EN ANALYSE
Zonder helder zicht op uw werk- en IT-omgeving plus de risico's en gevaren die beide (kunnen) bedreigen, kan u onmogelijk met succes de complexe beveiligingsarchitectuur voor zero trust security opzetten.

Gelukkig zorgen de investeringen die u doet in het opzetten van diezelfde architectuur, met name via de vijf pijlers, ook al voor een betere zichtbaarheid – van uw shadow IT, bijvoorbeeld, of van alle gebruikerstoestellen die u beheert (endpoint management).

Diezelfde investeringen leveren u ook heel veel data op. Daarop kan u vervolgens analyses uitvoeren om uw securityaanpak verder te verfijnen.

AUTOMATISERING EN ORKESTRATIE
Het spreekt voor zich dat u niet elke toegangscontrole eigenhandig kan uitvoeren. Hetzelfde geldt voor de meeste andere beveiligingstaken die we hier aanhaalden: microsegmentatie, encryptie, back-up … Daarom vereist een écht efficiënte securityaanpak dat u zoveel mogelijk taken automatiseert en software orkestreert.

GOVERNANCE
Zero trust security is geen eenvoudig, mooi afgebakend implementatieproject dat u tussendoor snel even kan afhandelen. Het is een complex traject voor strategische verandering op lange termijn, dat u continu moet opvolgen en regelmatig bijsturen. Daarom is het belangrijk dat u ook in goede governance voorziet, zodat u het nodige ownership over dat traject kan nemen en op elk moment het overzicht behoudt.

Zero trust security: bent u er klaar voor?

Bent u alvast gewonnen voor het concept van zero trust security, maar weet u niet meteen hoe u er het best mee van start kan gaan? Misschien heeft u zelfs uw eerste stappen al gezet op het pad naar zero trust security, maar twijfelt u nog over hoe het nu precies verder moet?

In beide gevallen bent u ongetwijfeld gebaat bij een korte studie of **security assessment**. Daarin maken wij een stand van zaken voor u op en brengen we ook uw **maturiteit** of **zero trust readiness** in kaart. Zo weet u tenminste al waar u staat.

Combineert u die instapoefening vervolgens met het opstellen van een **security roadmap**, die naast een stappenplan en **prioriteitenbeoordeling** ook concreet **technologieadvies** bevat, dan krijgt u meteen ook een heldere kijk op het vervolg van uw parcours. Zo weet u niet alleen waar u precies naartoe moet, maar ook hoe u er het best kan geraken.

SAMEN MAKEN WIJ ER WERK VAN!

Interesse in onze studies of assessments? Of heeft u voor uzelf die oefeningen al gemaakt, maar kijkt u uit naar een **ervaren technologiepartner** die u kan bijstaan bij het zetten van een aantal **gerichte stappen** naar zero trust security?

In beide gevallen kan u bij ons aankloppen. Voor alle technologische pijlers en fundamenten die in dit document aan bod komen, hebben wij de nodige expertise in huis.

Samen maken wij zo werk van een veiligere werkomgeving!

NEEM CONTACT OP

Inetum-Realdolmen
A. Vaucampslaan 42
1654 Huizingen, Belgium
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum realdolmen
Positive digital flow