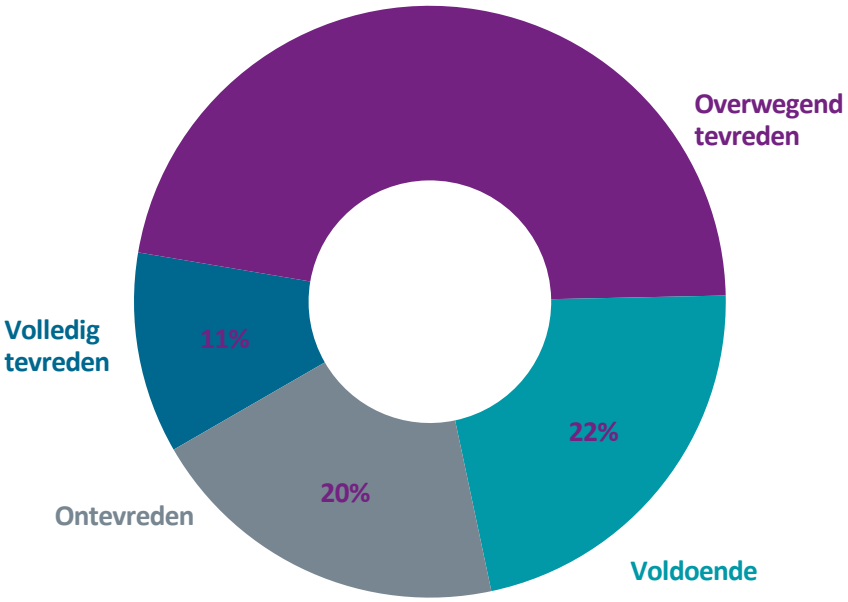
STATE OF CYBERSECURITY 2022: Benelux

Het bedrijfsleven heeft zich het afgelopen jaar aangepast aan de lessen die zijn geleerd uit de COVID-pandemie. Op personeelsniveau worstelen bedrijven met het vinden van de beste manieren om de flexibiliteit van werknemers en de bedrijfscultuur met elkaar in evenwicht te brengen. Op technisch niveau worden de vele voordelen van een cloud-first-architectuur afgewogen tegen de uitdagingen van het managen van complexiteit en de kosten in een multi-cloud-omgeving. Het gaat nog jaren duren voordat we begrijpen hoe de balans zal zijn in de post-pandemische omgeving, maar de eerdere veranderingen wijzen op een aanzienlijke herstructurering.

Een andere prominente takeaway van de pandemie is dat de symptomen vaak gemakkelijker te diagnosticeren en te behandelen zijn dan de hoofdoorzaken. Dit heeft uiteraard verwikkelingen die verder gaan dan bedrijfsstrategieën, maar een goed voorbeeld van dit concept in het bedrijfsleven is het gedeelte cybersecurity. Bedrijven worden maar al te bewust gemaakt van niet juist geconfigureerde cybersecurity wanneer ze zijn getroffen door een cyberaanval, en achteraf worden processen of tools geidentificeerd die de aanval zouden hebben kunnen voorkomen of geminimaliseerd hebben. Maar dat zal wellicht niet de onderliggende problemen aanpakken die kunnen leiden tot een ander cyberincident in de toekomst.

Het rapport 2022 State of Cybersecurity van CompTIA onderzoekt de ontbrekende verbinding tussen hoofdoorzaken en de symptomen. Digitale transformatie, gedreven door cloud- en mobiele adoptie, dwingt tot een nieuwe strategische aanpak van cybersecurity, maar het volledig overnemen van deze nieuwe aanpak brengt aanzienlijke uitdagingen met zich mee, zowel tactisch als financieel. Hoewel cybersecurity nog steeds een van de meest urgente kwesties voor moderne bedrijven is, maken de hindernissen die voortkomen uit de erfenis van de opvattingen over IT en een laag begrip van het dreigingslandschap, het moeilijk om de voorgeschreven werkwijze te volgen.

Tevredenheid organisatorische cybersecurity



CompTIA

INTEGRATIE VAN EEN 'ZERO TRUST'-AANPAK

Het gedeelte van cybersecurity is in veel opzichten een reactie op de manier waarop enterprise IT evolueert. De behoefte aan cybersecurity ontstaat immers pas nadat de technologie is geïmplementeerd. Deze dynamiek is de afgelopen jaren geïntensiveerd, omdat bedrijven op een offensieve manier de technologie nastreven met de neiging om cybersecurity als een tweede rangs overweging te behandelen.

Een manier waarop cybersecurity de evolutie van enterprise IT weerspiegelt, is dat het in beide gevallen strategischer is geworden. Als het gaat om algemene IT, omarmen organisaties over het algemeen de overgang naar een meer strategische aanpak, zelfs als er onderweg enkele groeipijnen zijn. Cybersecurity daarentegen blijkt een grotere uitdaging als het gaat om het aannemen van een strategische mindset.

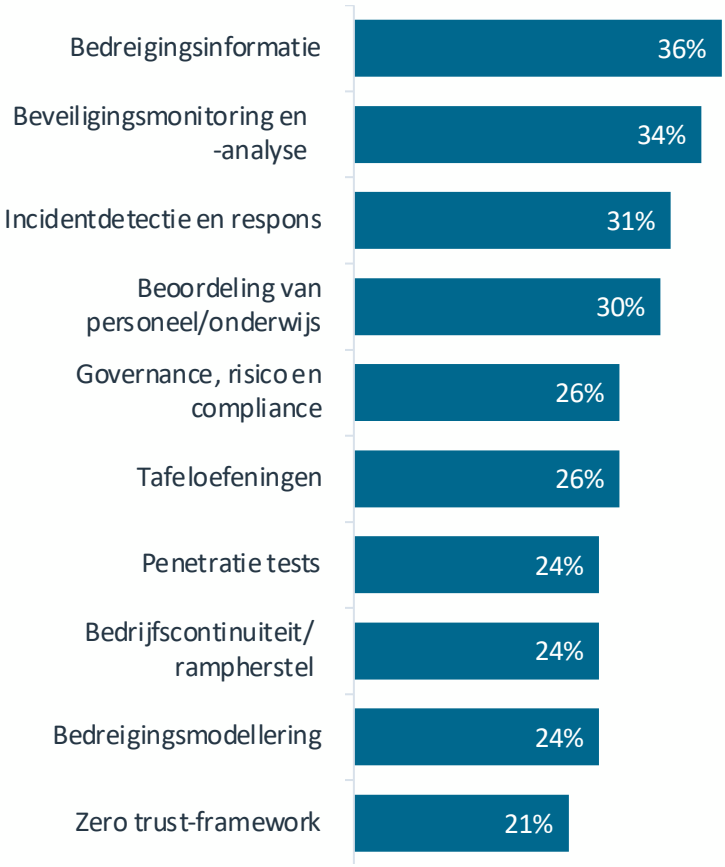
Een van de belangrijkste onderdelen van een strategische mindset is het besef dat cybersecurity niet meer primair gericht is op externe gebeurtenissen. Bij het onderzoeken van de kwesties die cybersecurity aandrijven, zijn de meeste van de belangrijkste kwesties extern gericht. De focus op volume, variatie of omvang van aanvallen is een focus op zaken die buiten het bedrijf gebeuren. Zelfs zorgen over privacy, zijn zorgen over externe verwachtingen. Er is minder erkenning dat cybersecurity samenhangt met de veranderende aard van interne operaties, zoals gegevens waar we steeds meer van afhankelijk zijn of de noodzaak om te blijven voldoen aan een veranderende regelgeving.

In het komende jaar zal er een gecentreerde verplaatsing plaatsvinden naar het integreren van cybersecurity met de bedrijfsvoering. Het accepteren van cybersecurity als een cruciaal onderdeel van digitale transformatie zal nieuwe vragen en nieuwe maatstaven van succes in de hele organisatie aansturen. Tegelijkertijd zal de vaststelling van een holistisch standpunt veel van de bestaande hindernissen rond het veranderen van de aanpak van cybersecurity aanpakken.

De introductie van cloud computing en mobiele apparaten veranderde drastisch het gezichtspunt van een veilige perimeter, die al tientallen jaren de dominante mindset was. Terwijl organisaties worstelden met de paradigmaverschuiving, was een moeilijk deel het definiëren van een alomvattende aanpak dat een breed scala aan cyberbeveiligings beslissingen informeerde. Zero trust bleek het antwoord op dat dilemma.

Dit jaar begint zero trust te verschuiven van een uitgebreid beleid naar tactische processen. Om verschillende redenen zal de invoering van zero trust niet van de ene op de andere dag plaatsvinden. Zero trust is in de eerste plaats een drastisch andere manier van denken over cybersecurity. In plaats van cybersecurity te zien als een van de vele componenten binnen de IT-functie en simpelweg te investeren in hardware of software, moeten bedrijven cybersecurity nu zien als een organisatorische noodzaak, die verder reikt dan technologische producten in beslissingen rond workflow en personeel.

Cybersecurity-praktijken op hun plaats



Zero trust is niet één product of actie, veel discrete tools en praktijken kunnen deel uitmaken van een aanpak van zero trust. Als we kijken naar componenten die doorgaans onder een zero trust-paraplu vallen, zijn er meer organisaties die individuele onderdelen herkennen dan het collectieve geheel zien. Multifactor authenticatie, een van de beste tools om vertrouwde identiteit te valideren, is aanwezig bij 29% van de organisaties. Cloud workload governance, een proces dat ervoor zorgt dat cloudbronnen volgens plan worden gebruikt, is aanwezig bij 26% van de organisaties. Andere elementen, zoals softwaregedefinieerde microsegmentatie (33%) en toegang met de minste privileges (23%), overtreffen ook het brede bewustzijn voor een zero trust-beleid.

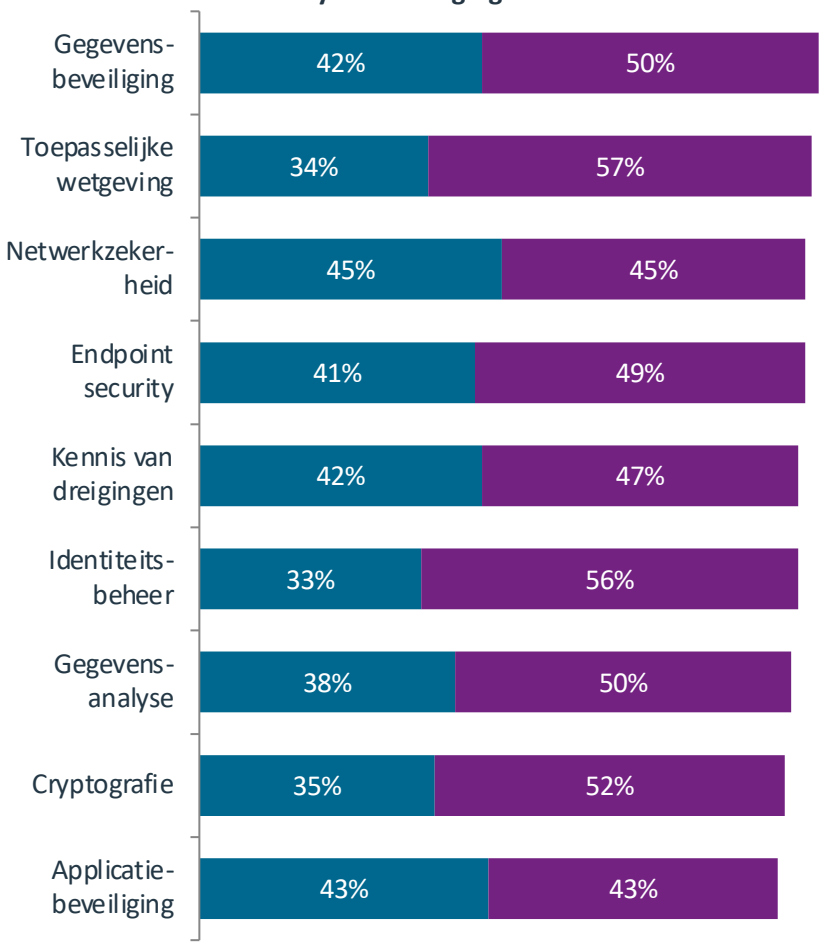
De belangrijkste conclusie is dat zero trust een filosofie is die het mogelijk maakt goed geïnformeerde vragen te stellen en goed geïnformeerde beslissingen te nemen. De beste manier om zero trust toe te passen, is niet om een reeks criteria te definiëren die op volledig succes wijzen, maar om een routekaart op te stellen met de stappen die het beste genomen kunnen worden basis van hoe de organisatie er bij staat. Deze stappen kunnen bestaan uit een volledige audit van gegevens en workflow, implementatie van specifieke producten zoals IAM-software (Identity and Access Management) of het opzetten van een doorlopend educatief programma voor het personeel. Elke stap moet een specifieke vraag behandelen en elke stap moet meetbare resultaten hebben.

MENSEN EN PRODUCT VERBINDEN naar een STRATEGIE

Als bedrijven proberen de onderliggende oorzaak van hun veiligheidstekortkomingen aan te pakken, ontdekken ze dat het probleem meerdere lagen heeft. Er is natuurlijk de technische laag, die al jaren het brandpunt is en nog steeds een substantieel onderdeel is van een cybersecurity-oplossing. Er is ook de workforce-laag, en veel bedrijven hebben zich gewend tot educatie om bewustwording van cybersecurity te verbeteren. Andere lagen die zich bezighouden met bedrijfsvoering en bedrijfsmetingen hebben de afgelopen jaren waarschijnlijk minder aandacht gekregen.

Aangezien bedrijven zich richten op het cultiveren van de cybersecurity-keten om zodoende alle lagen van de organisatie te omvatten, zullen technische specialisten altijd een cruciaal onderdeel zijn. Na een grondig onderzoek van vaardigheidstekorten is het verbeteren van vaardigheden de volgende uitdaging. Netwerkbeveiliging lijkt misschien een gebied met verdergaande expertise, sinds de taak al lange tijd wordt uitgevoerd, maar de realiteit is dat veranderingen in het IT-landschap constante verbetering vereisen. Andere gebieden zoals threat knowledge, data-analyse en identiteitsbeheer zijn meer voor de hand liggende kandidaten voor groei in vaardigheden, omdat ze recentere trends in cybersecurity vertegenwoordigen.

Behoefte aan vaardigheden op het gebied van cyberbeveiliging



De productlijst voor cybersecurity begint met items die al lang bestaan. Firewalls, antivirus en anti-malware waren de primaire componenten van de beveiligde perimeter, en ze dienen nog steeds die functie, zelfs als de beveiligde perimeter is gedaald in belangrijkheid. Deze tools zijn alom tegenwoordig, hoewel veel eindgebruikers (en mogelijk zelfs IT-personeel) ze misschien niet als onderdeel van de productenset beschouwen, omdat ze zo 'standaard' zijn.

Netwerkmonitoring is een ander hulpmiddel met een lange geschiedenis en evolueert om in de tijd te passen. Tools zoals SolarWinds Network Performance Monitor, Datadog Network Monitoring en Auvik bieden uitgebreide mogelijkheden voor het observeren en analyseren van een volledige netwerkarchitectuur. Recente functies in netwerkmonitoren omvatten inzicht in cloudcomponenten van het netwerk en analytische tools om inzicht in de gegevensstroom beter te begrijpen.

Door het belang van cloudsystemen te benadrukken, winnen SaaS-monitoring- en beheertools snel aan kracht. Versnelling in cloudadoptie was een van de grootste verschuivingen in IT-activiteiten tijdens de pandemie en bedrijven reageren nu op de tweedelijns effecten van die activiteit. Samen met cybersecurity problemen, komen cloud-systemen met een uniek aantal bedenkingen over het gebruik en de kosten en daarnaast nieuwe managementsoftware nodig is om cloud-architectuur goed te beheren, dirigeren en beveiligen.

Aan de andere kant van het spectrum zijn er tools die nog steeds lage acceptatiepercentages hebben, maar sterk moeten worden beschouwd als op handen zijnde toevoegingen. Hoewel SaaS de meest populaire vorm van cloud adoptie is, komt IaaS ook veel voor en kan het kritischer zijn voor een goede monitoring en beheer. Uitgebreide tools voor netwerk monitoring zijn cruciaal voor het verstrekken van een overzicht van het grote geheel, maar packet sniffers en LAN-analysatoren zijn gerichte producten die moeilijk te vinden problemen kunnen uitroeien.

Met zoveel tools in het arsenaal en zoveel beperkingen voor cybersecurity-personeel, is de voor de hand liggende volgende stap, automatisering. Automatisering kruist door de complexiteit van adoptie van meerdere producten, maar het hoeft niet per se de noodzaak voor cybersecurityspecialisten teniet te doen. Nieuwe expertise is nodig om automatisering goed te implementeren en doorlopende aanpassingen uit te voeren waar dat nodig is.

Zelfs als automatisering het resourceprobleem niet volledig oplost, maakt het de situatie beter beheersbaar. Het integreren van cybersecurity met bedrijfsvoering maakt cybersecurity nog belangrijker dan ooit en het implementeren van een zero trust-filosofie leidt tot een reeks nieuwe processen. Een toegewijde organisatiestructuur en de juiste toolset zijn de eerste stappen in het aanpakken van toegevoegde complexiteit. Door een evenwichtige benadering van automatisering te hanteren, kunnen organisaties hun onderliggende problemen volledig aanpakken en evolueren naar een gezond cybersecurity vooruitzicht.