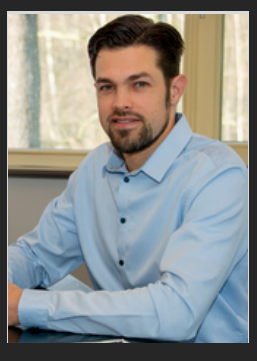
Editie 033
Juli 2024
SCHOTEN, Belgium

TECH TALK

"Insider Tips om je bedrijf sneller, eenvoudiger en winstgevender te laten lopen."

INSIDE THIS ISSUE:



Wij houden van technologie en we helpen graag mensen.
Bel me vandaag nog voor een kort (niet-verkoopgericht) gesprek om te ontdekken of mijn team en ik je kunnen helpen je gegevens beter te beveiligen en meer uit je bestaande technologie te halen!
- Jan Keersmaekers
Zaakvoerder

EEN EENVOUDIGE GIDS VOOR HET GEÜPDATETE NIST 2.0 CYBERSECURITY FRAMEWORK

Voor organisaties van elke grootte is het een uitdaging om bedreigingen voor te blijven. Het aantal gemelde wereldwijde beveiligingsincidenten steeg tussen februari en maart 2024. Ze namen toe met 69,8%. Het is belangrijk om een gestructureerde aanpak van cybersecurity te hanteren. Dit helpt om je organisatie te beschermen.

Het National Institute of Standards and Technology (NIST) heeft een Cybersecurity Framework (CSF) ontwikkeld. Het biedt een sectoronafhankelijke aanpak voor beveiliging. Het is ontworpen om bedrijven te helpen hun cyberrisico's te beheren en te verminderen. Het framework is onlangs in 2024 geüpdatet naar NIST CSF 2.0.

CSF 2.0 is een uitgebreide update die voortbouwt op het succes van zijn voorganger. Het biedt een meer gestroomlijnde en flexibele benadering van cybersecurity. Deze gids is bedoeld om het framework te vereenvoudigen.

Inzicht in de Kern van NIST CSF 2.0

De kern van CSF 2.0 is de Core. De Core bestaat uit vijf gelijktijdige en continue functies. Deze zijn: Identificeren, Beschermen, Detecteren, Reageren en Herstellen. Deze functies bieden een strategisch overzicht van cyberrisico's. Dit maakt een dynamische aanpak mogelijk voor het aanpakken van bedreigingen.

Hier zijn de vijf Kernfuncties van NIST CSF 2.0.

- Identificeren – Deze functie houdt in dat de organisatie haar assets, cyberrisico's en kwetsbaarheden identificeert en begrijpt.
- Beschermen – De beschermfunctie richt zich op het implementeren van waarborgen. Deze bescherming is bedoeld om cyberrisico's af te schrikken, te detecteren en te verminderen.
- Detecteren – Vroege detectie van cyberincidenten is cruciaal om schade te minimaliseren. De detectiefunctie benadrukt het belang van detectie.
- Reageren – De reageerfunctie beschrijft de stappen die moeten worden genomen in het geval van een cyberincident.
- Herstellen – De herstelfunctie richt zich op het herstellen van normale operaties na een cyberincident.

Profielen en Niveaus: Het Framework Aanpassen. Het geüpdatete framework introduceert het concept van Profielen en Niveaus. Deze helpen organisaties hun cybersecuritypraktijken aan te passen. Ze kunnen deze afstemmen op hun specifieke behoeften, risicotoleranties en middelen.

PROFIELEN – Profielen zijn de afstemming van de Functies, Categorieën en Subcategorieën. Ze zijn afgestemd op de bedrijfsvereisten, risicotolerantie en middelen van de organisatie.

NIVEAUS – Niveaus bieden context over hoe een organisatie naar cyberrisico's kijkt en welke processen er zijn om die risico's te beheren. Ze variëren van Partieel (Niveau 1) tot Adaptief (Niveau 4).

Voordelen van het Gebruik van NIST CSF 2.0

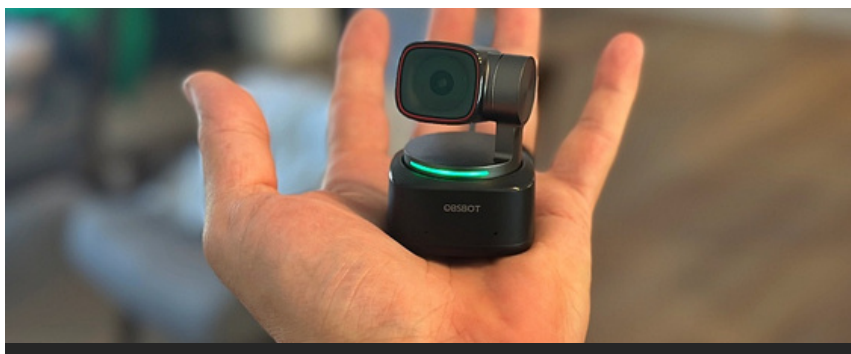
Verbeterde Cybersecuritypositie: Door de richtlijnen van NIST CSF 2.0 te volgen, kunnen organisaties een meer uitgebreid en effectief cybersecurityprogramma ontwikkelen.
Verminderd Risico op Cyberaanvallen: Het framework helpt organisaties om cyberrisico's te identificeren en te beperken.

- Verbeterde Naleving: NIST heeft CSF 2.0 afgestemd op veel industrienormen en -voorschriften.
- Verbeterde Communicatie: Het framework biedt een gemeenschappelijke taal om over cyberrisico's te communiceren.
- Kostenbesparingen: NIST CSF 2.0 kan organisaties helpen geld te besparen door cyberaanvallen te voorkomen.

Aan de Slag met NIST CSF 2.0

- Maak je vertrouwd met het framework
- Evalueer je huidige cybersecuritypositie
- Ontwikkel een cybersecurityplan
- Zoek professionele hulp

Door deze stappen te volgen, kun je beginnen met de implementatie van NIST CSF 2.0 in je organisatie. Tegelijkertijd verbeter je je cybersecuritypositie.



OBSBOT Tiny 2 4K Webcam

Verhoog je streaming- en videoconferentiespel met de OBSBOT Tiny 2 4K-webcam, die ongeëvenaarde functies biedt.

Hij heeft een 4K-resolutie, AI-tracking en een 2-assige gimbal die de video soepel houdt, ongeacht hoeveel je beweegt.

Upgrade vandaag nog je werkplek met de OBSBOT Tiny 2 en ervaar het verschil in videokwaliteit, trackingnauwkeurigheid en handsfree bediening.

Editie 033
Juli 2024
SCHOTEN, Belgium

VERLIEST JE BEDRIJF GELD OMDAT WN'S GEEN TECH KUNNEN GEBRUIKEN?

Gloednieuwe technologie kan opwindend zijn! Het belooft verhoogde efficiëntie, gelukkigere werknemers en een concurrentievoordeel. Maar die belofte kan een financiële nachtmerrie worden als je werknemerstraining en verandermgmt verwaarloost. Als werknemers moeite hebben om hun zakelijke tools te gebruiken, daalt de productiviteit. Fouten kunnen worden gemaakt en klantenservice kan eronder lijden.

Gebrek aan Tech Training

Stel je voor dat je investeert in een state-of-the-art CRM-systeem. Vervolgens zie je je verkoopteam worstelen in plaats van uitblinken. Ze kunnen geen belangrijke functies vinden, worstelen met gegevensinvoer en missen deadlines. Waarom? Omdat ze niet goed zijn opgeleid in de nieuwe software. Dit leidt tot de volgende kosten:

- Verloren Productiviteit
- Kostbare Fouten
- Demotivatie en Weerstand

Belang van change mgmt

Nieuwe technologie verstoort werkprocessen. Zonder goed verandermanagement voelen werknemers zich overweldigd en onzeker. Het doel is om hen succesvol te laten overgaan met goede training en ondersteuning. Wanneer bedrijven verandermanagement verwaarlozen, kunnen de volgende problemen ontstaan:

- Lage Moraal
- Gebruik van Shadow IT
- Weerstand tegen Toekomstige Verbeteringen

Bouw een succesverhaal

Dus, wat is de sleutel tot het ontsluiten van de ware waarde van nieuwe technologie? Het ligt in effectieve training en verandermanagement.

Hier is hoe je de negatieve kosten kunt vermijden en volledig kunt profiteren van je technologie:

=> Investeer in Uitgebreide Training - Behandel training niet als een bijzaak. Ja, sommige tools beweren dat ze gemakkelijk te gebruiken zijn. Maar mensen hebben verschillende niveaus van technische vaardigheden. Ontwikkel een op maat gemaakt trainingsprogramma dat verder gaat dan basisfuncties. Inclusief videotutorials, praktische workshops en doorlopende ondersteuningsmiddelen.

=> Richt je op Gebruikersadoptie, Niet Alleen op Funcies - Training moet niet alleen uitleggen hoe de software werkt. Het moet zich richten op hoe het nieuwe systeem de werknemers zal helpen in hun dagelijkse taken en de efficiëntie van de workflow zal verbeteren. Als werknemers de nieuwe oplossing niet omarmen, faalt het project.

=> Omarm Verandermanagement - Communiceer het "waarom" achter de verandering. Leg uit hoe de nieuwe technologie het werk van iedereen gemakkelijker zal maken. Moedig open communicatie aan en pak zorgen aan gedurende de overgangsperiode.

DE ESSENTIE
Nieuwe technologie is een krachtig middel, maar het is alleen waardevol als het goed wordt gebruikt. Geef prioriteit aan training en verandermgmt. Dit zal je helpen om de kloof te dichten tussen een glanzend nieuw systeem en een werkelijke return on investment. Gelukkige, goed opgeleide werknemers die de juiste tools gebruiken zijn je geheime wapen. Ze kunnen je helpen de efficiëntie te maximaliseren, de moraal te verhogen en voorop te blijven in de concurrentie.

GLOEDNIEUW OP DE DIGITALE PERS... ONTDEK MICROSOFT COPILOT VOOR FINANCIËN

MS Copilot voor financiën is een knaller in de wereld van bedrijfs-ai. deze app, aangedreven door genai, verschijnt in verschillende functionele activiteiten. de nieuwste toepassing is financiële processen.

Microsoft Copilot voor Financiën is baanbrekend. Het injecteert de kracht van AI van de volgende generatie in het hart van je dagelijkse werkstroom. Stel je voor dat je een AI-maatje hebt dat de complexiteiten van financiën begrijpt en naadloos met je samenwerkt.

Het kan een ervaren financieel analist of een nieuwsgierige leerling helpen. Het automatiseert repetitieve taken en biedt real-time inzichten. Copilot staat op het punt om te revolutioneren hoe we ons bewegen in het financiële domein.

WAT IS MICROSOFT COPILOT VOOR FINANCIËN?

Copilot voor Financiën is een nieuwe Copilot-ervaring in Microsoft 365. Het verbindt met bedrijfsfinanciële systemen zoals Dynamics 365 en SAP. Het biedt financiële inzichten en begeleide acties in:

- Outlook
- Excel
- Microsoft Teams
- Andere Microsoft 365-toepassingen

Voordelen van het Gebruik van Copilot voor Financiën

- Copilot voor financiën biedt verschillende voordelen voor mensen in financiële functies. Deze omvatten:
- Ontsnappen aan het Handmatige Werk
- AI-aangedreven Inzichten binnen Handbereik
- Op Maat gemaakt voor Jouw Team
- Naadloze Integratie voor een Frictieloze Ervaring
- Gebouwd met Vertrouwen in Gedachten

Een Blik in de Toekomst van Financiën
Copilot voor Financiën vertegenwoordigt een significante sprong voorwaarts in financiële technologie. Het gaat verder dan automatisering. Het draait om het benutten van de kracht van AI om menselijke expertise aan te vullen en de manier waarop financiën worden beheerd te transformeren.

10 STAPPEN RICHTING CULTUUR V CYBERBEWUSTZIJN

cyberaanvallen zijn een constante dreiging in de digitale wereld van vandaag. phishing e-mails, malware downloads en datalekken kunnen bedrijven lamleggen en persoonlijke levens verwoesten.
het opbouwen van een cultuur van cyberbewustzijn vereist geen complexe strategieën of dure trainingsprogramma's. hier zijn enkele eenvoudige stappen die je kunt nemen om een groot verschil te maken:

1. begin met steun van het management
2. maak beveiligingsbewustzijn leuk, niet angstig
3. spreek hun taal
4. hou het kort en krachtig
5. voer phishing-oefeningen uit
6. maak rapporteren gemakkelijk en aangemoedigd
7. beveiligingskampioenen: geef je werknemers kracht
8. buiten werk: beveiliging stroomt over
9. vier successen
10. maak gebruik van technologie

IPHONE TRAGER DAN ANDERS? VOLG DEZE TIPS

Laten we eerlijk zijn, iPhones zijn geweldige apparaten. Maar zelfs de meest gestroomlijnde, krachtige iPhone kan ten prooi vallen aan de gevreesde vertraging. Apps doen er eeuwen over om te laden en scrollen voelt traag aan. Al snel worden eenvoudige taken frustrerende beproevingen.

Als je iPhone van snelle hulp naar trage slak is gegaan, geen paniek!

Hier zijn een paar eenvoudige tips om je iPhone weer in topconditie te krijgen:

- Geef het een herstart: De digitale power nap
- Ruim de digitale rommel op
- Tem achtergrondapp-refresh
- Schakel locatiediensten uit waar mogelijk
- Verminder bewegingseffecten
- Update je apps en iOS
- Nucleaire optie: Reset je iPhone (Maak eerst een back-up!)
- Controleer de gezondheid van je batterij

WAAROM CONTINU MONITOREN EEN CYBERSECURITY MUST IS

Cyberdreigingen evolueren voortdurend, en traditionele beveiligingsmaatregelen zijn niet langer voldoende. Continue monitoring fungeert als jouw waakzame digitale bewaker. Het controleert voortdurend op zwakke plekken en slaat alarm voordat aanvallers er misbruik van maken. Hier is waarom continue monitoring een must is in cybersecurity:

- Snelle Inbreuken
- Geavanceerde Bedreigingen Vereisen Geavanceerde Verdedigingen
- Compliance-eisen schrijven het vaak voor
- Gemoedsrust en Lagere Kosten
- Verbeterde Nauwkeurigheid bij Bedreigingsdetectie
- Snellere Incidentrespons
- Verbeterde Beveiligingspositie
- Compliance Rapportage

In het huidige bedreigingslandschap is continue monitoring geen luxe. Het is een absolute noodzaak op het gebied van beveiliging.

Wacht niet tot een beveiligingsinbreuk je wakker schudt. Omarm continue monitoring en neem controle over je cybersecuritypositie. Een ounce preventie is een pond genezing waard, vooral in de digitale wereld.

TECHNOLOGIE TRIVIA TIME

De vraag van deze maand is:

Wat is de naam van dat schattige pinguïn karakter dat verschijnt in het Linux besturingssysteem?

Laat het ons weten :-)