

TECH INFO

PERIODIEKE UITGAVE VAN  TROTS IT



Veiligheid voor alles

Stoptober.... Pink Ribbonmaand....

De maand oktober staat jaarlijks in het teken van zaken die voor ons allemaal van levensbelang zijn.

Als partner van het overheidsinitiatief Alert Online voegen wij daar graag een motto aan toe. Een motto dat van levensbelang voor uw bedrijf kan zijn. Oktober is namelijk ook Europese maand van de Cyberveiligheid. In het leven roepen voor bewustwording rondom online veiligheid en het stimuleren van cybersecure gedrag.

Cyberawareness en cyberweerbaarheid zijn zaken die elke ondernemer op zijn agenda zou moeten hebben. En niet alleen in oktober. Wist u namelijk dat het merendeel van de cybersecurity-inbreuken bij bedrijven wordt veroorzaakt door menselijke fouten?

Daarom staat deze Tech Info in het teken van de cybersecuritymaand. Omdat ook bij Trots IT veiligheid voor alles gaat.

Oktober 2022



Deze uitgave is beschikbaar gesteld door Peter van der Linden, directeur Trots IT.

Onze Missie: bedrijfseigenaren in de Randstad met 100% toewijding en persoonlijke aandacht de meest betrouwbare en professionele IT ondersteuning bieden die mogelijk is.



6 Belangrijke IT-beleidsmaatregelen Die Elk Bedrijf Zou Moeten Toepassen

Oktober is Cybersecuritymaand. Een goed moment voor elk formaat bedrijf om eens kritisch te kijken naar de IT-beleidsregels die zij hanteren. Veel Mkb's maken de fout om het daar niet over te hebben. Ze vinden dat het allemaal niet zo formeel hoeft te zijn, vertellen het personeel gewoon wat er wordt verwacht als het ter sprake komt en gaan ervan uit dat dat voldoende is.

Maar deze manier van denken kan problemen veroorzaken voor Mkb-eigenaren. Medewerkers kunnen namelijk geen gedachten lezen. Dingen waarvan u denkt dat ze vanzelfsprekend zijn, zijn dat voor hen misschien niet. Als u geen beleid heeft, kan dit u zelfs juridische problemen opleveren zoals een rechtszaak wegens misbruik van een bedrijfsapparaat of e-mailaccount.

Wist u dat 77% van de werknemers tijdens het werk toegang heeft tot hun sociale media-accounts? 19% van hen besteedt bovendien gemiddeld een volledig uur per werkdag aan sociale media. In sommige gevallen negeren werknemers simpelweg het bedrijfsbeleid. Maar in andere gevallen is er geen specifiek omschreven beleid dat ze moeten volgen. IT-beleid is een belangrijk onderdeel van uw IT-beveiliging en technologiebeheer, hoe groot

uw bedrijf ook is. In dit artikel helpen we u op weg met enkele van de belangrijkste IT-beleidsregels.

Wachtwoordbeveiligingsbeleid

Meer dan driekwart van alle datalekken in de cloud is afkomstig van gecompromitteerde wachtwoorden. Gecompromitteerde inloggegevens zijn wereldwijd nu ook de grootste oorzaak van datalekken.

Een wachtwoordbeveiligingsbeleid bepaalt voor uw team hoe ze met hun inlogwachtwoorden moeten omgaan. Het moet dingen bevatten als:

- Hoe lang wachtwoorden moeten zijn
- Hoe wachtwoorden samen te stellen (bijvoorbeeld door ten minste één cijfer en symbool te gebruiken)
- Waar en hoe wachtwoorden op te slaan
- Het gebruik van multi-factor authenticatie (indien vereist)
- Hoe vaak wachtwoorden gewijzigd moeten worden.

Acceptable Use Policy (AUP)

Het Acceptable Use Policy is een overkoepelend beleid. Het beschrijft hoe u technologie en data op de juiste manier in uw organisatie moet gebruiken. Dit beleid regelt zaken als apparaatbeveiliging.

Vervolg op pagina 2

Vervolg van pagina 1

U wilt bijvoorbeeld dat medewerkers hun apparaten geüpdatet houden. Als dat zo is, moet u dat in dit beleid opnemen.

Iets anders wat u in uw AUP moet opnemen, is wat bij het gebruik van bedrijfsapparaten is toegestaan. U kunt bijvoorbeeld ook verbieden dat op afstand werkende medewerkers hun werkapparaten met gezinsleden delen.

Data is ook onderdeel van de AUP. Het moet bepalen hoe gegevens moeten worden opgeslagen en verwerkt. Het beleid vereist bijvoorbeeld een versleutelde omgeving voor beveiliging ervan.

Beleid Voor Cloud- & Appgebruik

Het gebruik van ongeautoriseerde cloudapplicaties door medewerkers is een groot probleem geworden. Geschat wordt dat het gebruik van deze 'schaduw-IT' varieert van 30% tot 60% van het cloudgebruik van een bedrijf.

Vaak gebruiken medewerkers uit eigen beweging cloud-apps omdat ze niet beter weten. Ze realiseren zich niet dat het gebruik van niet-goedgekeurde cloudtools een groot beveiligingsrisico voor bedrijfsdata is.

Een beleid voor cloud- en appgebruik vertelt werknemers welke cloud- en mobiele apps geschikt zijn om voor zakelijke gegevens te gebruiken. Het moet het gebruik van niet-goedgekeurde applicaties beperken en een manier bieden om veilige apps voor te stellen die de productiviteit kunnen verbeteren.

Bring Your Own Device (BYOD) Beleid

Ongeveer 83% van de bedrijven hanteert een BYOD-aanpak voor mobiel gebruik door werknemers. Door werknemers hun eigen smartphones voor het werk te laten gebruiken, besparen bedrijven geld. Het kan ook handiger voor werknemers zijn, omdat ze zo geen tweede mobiele telefoon bij zich hoeven te hebben.

Maar als u geen beleid heeft dat het gebruik van BYOD bepaalt, kunnen er beveiligings- en andere problemen ontstaan. Apparaten van werknemers kunnen kwetsbaar zijn voor aanvallen als het besturingssysteem niet wordt bijgewerkt. Ook kan er verwarring ontstaan over vergoedingen voor het gebruik van persoonlijke apparaten voor werk.

Het BYOD-beleid verduidelijkt dergelijke zaken. En kan bijvoorbeeld ook de vereiste installatie van een app voor eindpuntbeheer bevatten.

Beleid Voor Wifi-gebruik

Openbare wifi is een groot probleem met betrekking tot cyberbeveiliging. 61% van de ondervraagde bedrijven zegt dat werknemers verbinding maken met openbare wifi vanaf apparaten die eigendom zijn van het bedrijf.

Veel werknemers staan niet stil bij het inloggen op een bedrijfsapplicatie of e-mailaccount. Zelfs niet als dat via een openbare internetverbinding gebeurt. Dit kan hun inloggegevens echter blootleggen en tot een inbreuk op uw bedrijfsnetwerk leiden.

In uw beleid voor wifi-gebruik wordt uitgelegd, hoe werknemers ervoor moeten zorgen dat ze veilige verbindingen hebben. Het kan het gebruik van een bedrijfs-VPN voorschrijven of de activiteiten bij het gebruik van openbare wifi beperken. Zoals het niet kunnen invoeren van wachtwoorden of betaalkaartgegevens in een formulier.

Beleid Voor Gebruik Van Sociale Media

Nu het gebruik van sociale media op het werk steeds normaler is, is het belangrijk om hier in uw beleid ook iets mee te doen. Anders zou eindeloos scrollen en posten elke week uren aan productiviteit kunnen kosten.

Neem details op in uw socialemediabeleid, zoals:

- Beperken wanneer werknemers toegang hebben tot persoonlijke sociale media
- Beperken wat werknemers over het bedrijf kunnen posten
- Vermeld 'veilige selfie-zones' of ruimtes die niet geschikt zijn voor openbare afbeeldingen

Vraag Hulp Om De Documentatie Van Uw IT-beleid & Veiligheid Te Verbeteren

Vindt u Oktober Cybersecuritymaand ook een goed moment om eens kritisch naar uw IT-beleid te kijken? Wij helpen uw bedrijf graag deze te verbeteren en beveiligingsproblemen aan te pakken. Neem vandaag nog contact met ons op om een afspraak in te plannen en samen aan de slag te gaan.



Heeft U Momenteel Inzicht In Hoe Veilig, Stabiel En Efficiënt Uw IT-systemen Zijn?

Als het antwoord "NEE" is – zoals bij het merendeel van de Mkb'ers in Nederland – dan stelt u uzelf en uw bedrijf mogelijk bloot aan **enorme aansprakelijkheid, hoge boetes en gemiste kansen, rechtszaken, diefstal** en nog veel meer.

Waarom? Omdat u het belangrijkste doelwit van een hacker bent. Ze weten dat u toegang heeft tot financiële gegevens, personeelsdossiers, bedrijfsgegevens en interessante informatie zoals burgerservicenummers, creditcardnummers, geboortedata, thuisadressen, e-mailadressen et cetera.

Maakt u zich zorgen hierover? Blijf er niet mee zitten, maar maak gebruik van ons aanbod voor een betrouwbare externe beoordeling van uw situatie op een volledig kosten- en risicovrije manier.

Plan Vandaag Nog Onze 100% vrijblijvende 10-Minuten Analyse In!

Aan het einde van de beoordeling weet u:

- Of uw systemen en gegevens echt zijn beveiligd tegen hackers en ransomware en waar u gedeeltelijk of volledig kwetsbaar bent.
- Of er daadwerkelijk een back-up van uw gegevens wordt gemaakt waarmee u in geval van nood of een ransomware aanval snel weer in bedrijf bent.
- Waar u zonder het te weten mogelijk de AVG-wetgeving overtreedt.
- Hoe u de communicatie, beveiliging en prestaties kunt verbeteren, evenals de securitykennis van uw medewerkers.

Een frisse blik ziet dingen die u voorheen wellicht over het hoofd zag.

Reserveer daarom vandaag nog uw 10-Minuten Analyse via

<https://www.trotsit.nl/nl/10-minuten-analyse/>

TROTS IT IN HET NIEUWS

Trots IT En Holm Security Partners In Online Veiligheid Ondernemers

Onlangs zijn wij met het internationale cybersecuritybedrijf Holm Security een samenwerking op het gebied van risico- en kwetsbaarheidsmanagement aangegaan. Het doel van dit partnerschap is met name om het dienstenpakket op het gebied van cybersecurity voor de IT-omgevingen van onze klanten nog verder te versterken.

Transparantie en inzicht

Als leverancier van multinational-level IT-security & -beheer voor het Mkb met een focus op de veiligheid en continuïteit van de bedrijfsnetwerken zien wij de tools van Holm Security voor het scannen van systemen, netwerken en webapplicaties als een waardevolle aanvulling op onze diensten. Deze samenwerking biedt onze klanten de mogelijkheid om een onafhankelijke, externe bevestiging van de werking van onze producten en diensten te krijgen. Het geeft ze zo volledige transparantie en inzicht in hoe veilig hun netwerken en data daadwerkelijk zijn.

Trainen tegen phishing-aanvallen

Bewustzijn van medewerkers en het herkennen van online inbreukpogingen wordt steeds belangrijker. 95% van de kwetsbaarheden ontstaat namelijk door menselijke fouten. Daarom omvat de samenwerking met Holm Security ook mogelijkheden voor phishing & awareness trainingen, waarmee werkgevers de zwakke plekken ontdekken en medewerkers leren waar ze alert op moeten zijn.

Wie meer wil weten over deze samenwerking en de mogelijkheden voor de IT-omgeving, kan contact met ons opnemen via info@trotsit.nl of bellen naar 088-2055888.

HET BELANGRIJKSTE WOORD IN HET BEDRIJFSLEVEN



“Wat is de belangrijkste mindset voor zakelijk succes?”

Deze vraag werd mij onlangs gesteld door een videopodcaster en ik heb zorgvuldig nagedacht over mijn antwoord. Aanvankelijk dacht ik dat het niet mogelijk was om de meest belangrijke mindset vast te stellen. Ik vind dat vragen die maar om ‘één ding’ gaan, geneigd zijn om de zaak te veel te vereenvoudigen. Ik vond dat succes meestal afhangt van meerdere factoren en niet kan worden onderverdeeld in één enkele denkrichting, maar plotseling drong het tot me door: de enige mindset die ik ontelbare keren bij succesvolle ten opzichte van onsuccesvolle ondernemers heb waargenomen, is vrijgevigheid.

Vaak zie je dat bedrijven eerlijkheid als hun belangrijkste kernwaarde beschouwen, maar naar mijn mening is dat nogal laag ingezet. Bedrijven zouden hun werknemers er niet aan hoeven herinneren niet oneerlijk te zijn. Andere bedrijven stellen vriendelijkheid voorop, maar vriendelijkheid voegt eigenlijk niets toe aan het leven van hun klanten.

Bedrijven die respect als hun mindset stellen, zijn op de goede weg maar missen nog steeds de voordelen die vrijgevigheid met zich meebrengt. Door iemand vrijgevigheid te tonen, geef je ze respect terwijl je ze ook iets waardevols geeft. Als je er echt over nadenkt, zijn leiders die slagen vaak genereus. Ze zijn in

staat om hun werknemers, hun klanten, hun aandeelhouders en de gemeenschap te behandelen met een gevoel van ruimhartigheid dat hen succes brengt. Degenen die dit niet tonen, slagen op de lange termijn zelden. Tijdens mijn loopbaan heb ik veel ondernemers ontmoet die succes en mislukking hebben meegemaakt door hun generositeit.

Ik sprak ooit met de CEO van een hypotheekverstrekker die suggereerde dat zijn bedrijf succes had door huiseigenaren met een laag inkomen te ‘misleiden’ om hypotheeken met verborgen, ongunstige voorwaarden aan te gaan. Toen in 2008 de huizencrisis toesloeg, maakte een stapel rechtszaken een einde aan het bedrijf en de carrière van deze man.

Ik herinner me daarentegen een gesprek met Ted Waite, een van de mede-oprichters van Gateway. Ik stond versteld dat een man als Ted, een cowboy in een gescheurde spijkerbroek, middenin South Dakota een computerproductiebedrijf van miljarden dollars kon oprichten. Ted hield ervan om technologie voor zijn klanten minder stressvol te maken, terwijl hij mensen waar voor hun geld gaf. Zijn geest van vrijgevigheid werd weerspiegeld in zijn bedrijfscultuur.

We denken vaak dat we er alles aan moeten doen om meer geld binnen te halen, maar een vrijgevege mindset aannemen is beter als je succes in het leven en in je carrière wilt hebben.



Dr. Geoff Smart is de directeur en oprichter van ghSMART, een adviesbureau voor leiderschap dat leiders helpt hun positieve impact op de wereld te vergroten. Dr. Smart en zijn firma hebben meerdere New York Times-bestsellers gepubliceerd. Hij blijft actief in zijn gemeenschap en heeft veel overheidsfunctionarissen geadviseerd.



OKTOBER CYBER SECURITY MAAND

Oktober is Cybersecuritymaand. Een jaarlijks terugkerende campagne vanuit de overheid waarin aandacht wordt gevraagd voor bewustwording rondom online veiligheid en het stimuleren van cybersecure gedrag.

Als partner van Alert Online - een gezamenlijk initiatief van overheid, bedrijfsleven en wetenschap - ondersteunen wij deze campagne van harte. Want ook Trots IT is continu bezig zijn zakelijke klanten bewust te laten zijn van de risico's en te helpen bij hun cyberweerbaarheid. Sowieso zijn al onze diensten en tools ingericht op veiligheid en continuïteit. Maar menselijke fouten vormen een groot aandeel, waar het gaat om datalekken en inbreuken op bedrijfsnetwerken.

Jaarlijks onderzoek online risico's

In het kader van deze Cyber Security Maand doet Alert Online jaarlijks op verzoek van het ministerie van Economische Zaken en Klimaat, directie Digitale Economie onderzoek naar de kennis over en beleving van online risico's. Daaruit bleek dat men zich over de gehele linie minder zorgen maakt over hun online veiligheid dan in het afgelopen jaar. Maar is dat terecht? Enkele cijfers uit het onderzoek:

- Phishing blijft de meest ervaren vorm van cybercrime, gevolgd door hulpvraagfraude, malware en hacking.
- Hulpvraagfraude en hacking worden ten opzichte van vorig jaar vaker genoemd.

- Slechts drie op de tien Nederlanders weet wat social engineering is.
- Bijna de helft van de ondervraagden vindt het hebben van verschillende wachtwoorden voor apparaten en online accounts te veel gedoe.
- Een op de vijf medewerkers ontving in de afgelopen 12 maanden op het werk een phishingmail.
- Een kwart van de kleine bedrijven onderneemt geen actie om veilig online te zijn.

Wilt u weten waar u staat qua cybersecure gedrag? Kijk eens op veiliginternetten.nl voor meer informatie over de campagne van Alert Online en bewustwording rondom online veiligheid.



MAAK UW VERGADERINGEN PRODUCTIEVER

Als ondernemer bent u waarschijnlijk elke dag aan het vergaderen. Dergelijke meetings kunnen al snel tijdrovend worden, als er voor-

af geen concreet plan is. Geeft u altijd leiding aan deze vergaderingen? Dan kunt u het volgende doen om ervoor te zorgen dat ze zo productief mogelijk zijn.

- Nodig alleen de noodzakelijke personen en teams voor de vergadering uit. Het heeft geen zin om elke medewerker bij elke vergadering te hebben.
- Maak een agenda om te voorkomen dat uw vergadering ontspoord of te veel uitloopt. Stuur deze agenda voorafgaand aan de vergadering naar de relevante personen en hou het gesprek volgens een stappenplan gaande.
- Bepaal een begin- en eindtijd om uw werkdag op schema te houden. Zo weten uw medewerkers dat u ook hun tijd kostbaar vindt.
- Plan de vergadering op een moment waarop iedereen alert en er klaar voor is om het betreffende onderwerp te bespreken. Maak ook gebruik van een notulist zodat uw team later kan teruglezen wat er is besproken voor het geval ze iets hebben gemist.
- Stel deadlines in en maak tijdens de vergadering een actieplan voor uw team. Dit schept verantwoordelijkheid, zodat u zeker weet dat iedereen oplet en zijn of haar taken op zich neemt.