

TECH INFO

DECEMBER 2022

IT tips om
uw bedrijf
vooruit te
helpen!



Eindejaarsbeoordeling van uw IT-Infrastructuur? Dit Moet er Zeker in!

Het einde van het jaar is altijd het perfecte moment om plannen te maken voor de toekomst. De meeste bedrijven hopen bij een nieuw jaar op groei en verbetering van de bedrijfsvoering. Een groot deel van die bedrijfsvoering is afhankelijk van technologie. Logisch dus, om voor verbeteringen ook naar uw IT te kijken.

Een eindejaarsbeoordeling van de technologie biedt u de mogelijkheid om verschillende aspecten van uw IT onder de loep te nemen. Neem de tijd om te focussen op verbeteringen die uw winst een boost geven. Maar ook welke tactieken u moet inzetten om het risico op een kostbare cyberaanval te verkleinen.

Deloitte keek in een recent onderzoek naar digitaal vooruitstrevende Mkb'ers. Daaruit bleek dat Mkb'ers die slim gebruik maken van technologie hoger scoren dan hun branchegenoten. Onder andere met:

- 2x zoveel omzet per medewerker
- Omzetgroei jaar op jaar die bijna 4x zo hoog is
- Gemiddelde personeelsgroei van meer dan 6x zo hoog

Bedrijven die technologie goed gebruiken, doen het dus beter. En ze zijn bovendien veiliger. Volgens IBM verlagen bedrijven die een actieplan voor incidenten hebben de kosten van een datalek met 61%.

Neem in de laatste weken van dit jaar even de tijd om samen met uw IT-medewerkers of externe IT-bedrijf een technologiebeoordeling uit te voeren. Dan bent u klaar voor succes en veiligheid in het komende jaar.

Aandachtspunten Bij Uw Eindejaarsbeoordeling

Het doel van zo'n eindejaarsbeoordeling is om naar

alle gebieden van uw IT-infrastructuur te kijken. Beveiliging, efficiëntie en basisoverwegingen zullen de belangrijkste aanjagers zijn voor toekomstige acties.

IT-beleid

Wanneer het IT-beleid verouderd raakt, houden mensen zich er niet meer aan. Bekijk al uw beleidsregels om te zien of ze aan de nieuwe criteria moeten worden aangepast. Als u momenteel bijvoorbeeld een deel van het personeel thuis laat werken, zorg er dan voor dat uw gebruiksbeleid voor apparaten dit weer spiegelt.

En laat het uw werknemers weten wanneer het beleid is bijwerkt. Dit biedt ze een opfrismoment voor belangrijke informatie, die mogelijk wat is weggezaakt.

Disaster Recovery Plan

Wanneer heeft uw bedrijf voor het laatst een incident response oefening gedaan? Is er een lijst met stappen die werknemers moeten volgen in het geval van natuurgeweld of een cyberaanval?

Neem de tijd om de disaster recovery planning voor het nieuwe jaar te bekijken. U moet ook momenten inplannen voor rampenoefeningen en trainingen in de komende maanden.

IT Problemen & Pijnpunten

U wilt geen grote IT-upgrade ondergaan zonder daarin de pijnpunten van werknemers mee te nemen. Anders mist u misschien een aantal gouden kansen om de productiviteit en het welzijn van het personeel te verbeteren.

Doe een onderzoek naar hoe uw werknemers technologie gebruiken. Stel vragen over hun favoriete en

minst favoriete applicaties. Vraag met welke problemen ze te maken hebben. Laat ze u vertellen hoe technologie volgens hen zou kunnen verbeteren om hun werk beter te doen. Dit komt uw bedrijf weer ten goede. Het kan u ook helpen verbeteringen door te voeren, die de meest impact hebben.

Bevoorrechte Toegang & Ongebruikte Accounts

Controleer tijdens uw eindejaarsbeoordeling de accounts met hogere rechten. Na verloop van tijd kunnen machtigingen worden misbruikt. Hierdoor loopt uw netwerk een groter risico op een ernstige aanval.

Zorg ervoor dat alleen degenen die ze nodig hebben, machtigingen op beheerdersniveau hebben. Hoe minder accounts met hogere rechten u in uw bedrijfstools heeft, hoe lager uw risico. Een gecompromitteerd wachtwoord voor accounts met hogere rechten opent de deur naar grote schade.

Zoek tijdens het doornemen van uw accounts ook naar ongebruikte accounts en sluit ze af. Als u ze actief laat, vormt dit een beveiligingsrisico.

Op onze website behandelen wij nog meer zaken zoals cloudgebruik en schaduw-IT. Ga naar www.trotsit.nl/nieuws voor alle aandachtspunten die belangrijk zijn om mee te nemen in uw eindejaarsbeoordeling.

Plan Vandaag Nog Een IT- & Beveiligingsanalyse In!

We kunnen u helpen met een grondige evaluatie van uw IT-omgeving om u een actieplan voor een veiligere toekomst te geven. Neem vandaag nog contact met ons op voor een gratis consult.

OBSTAKELS VOOR BYOD OVERWINNEN

Mobiele apparaten vormen ongeveer 60% van de endpoints in een bedrijfsnetwerk. En zo'n 80% van de werkzaamheden gaat via deze apparaten.

Maar op het gebied van strenge cyberbeveiligingsmaatregelen worden ze vaak genegeerd. Dit geldt met name voor mobiele apparaten die eigendom zijn van werknemers.

De aanschaf van telefoons en abonnementen voor personeel is financieel vaak onhaalbaar. Bovendien kan het voor werknemers lastig zijn om altijd twee verschillende apparaten bij zich te hebben.

Reden voor ongeveer 83% van de bedrijven om de voorkeur te geven aan BYOD (Bring Your Own Device), het gebruik van privé smartphones, laptops en tablets voor werk.

Hier zijn enkele tips om de veiligheid en uitdagingen van BYOD op te lossen.

Definieer uw BYOD-beleid

Als er geen vastgestelde regels zijn voor BYOD, kunt u niet verwachten dat het gebruik veilig gebeurt. Medewerkers kunnen bedrijfsgegevens onbeschermd achterlaten. Of ze maken verbinding met openbare wifi en voeren vervolgens hun zakelijke e-mailwachtwoord in, waardoor het voor anderen zichtbaar wordt.

Als u werknemers vanaf persoonlijke apparaten toe-

gang geeft tot zakelijke gegevens, heeft u een beleid nodig. Het beschermt uw bedrijf tegen onnodige risico's.

Houd uw Beleid Actueel

Zodra een beleid verouderd raakt, wordt het minder relevant voor medewerkers en zijn ze geneigd het te negeren. Zorg er dus voor dat u uw BYOD-beleid regelmatig bijwerkt.

Gebruik VoIP voor Zakelijke Gesprekken

Als klanten persoonlijke nummers van medewerkers hebben, kan dat voor problemen zorgen. Medewerkers die het bedrijf verlaten, zullen dergelijke oproepen mogelijk niet meer beantwoorden. En de klant begrijpt vervolgens niet waarom.

Met een zakelijk VoIP-telefoonstelsel kunt u dit probleem voorkomen. Deze diensten hebben mobiele applicaties die werknemers kunnen gebruiken.

Met mobiele VoIP-apps kunnen werknemers via een bedrijfsnummer bellen en gebeld worden.

Stel Beperkingen in voor het Opslaan van Bedrijfsgegevens

Ongeacht het type apparaat moet u altijd de controle over uw bedrijfsgegevens behouden.

Het is verstandig om de soorten gegevens te beper-

ken die medewerkers op persoonlijke apparaten kunnen opslaan.

Zorg er ook voor dat er een back-up van uw bedrijfsgegevens vanaf die apparaten wordt gemaakt.

Verplicht Apparaatupdates

Wanneer apparaten van werknemers niet worden bijgewerkt of gepatcht, is dat vragen om een datalek. Elk eindpunt dat verbonden is met uw netwerk kan een inbreuk mogelijk maken. Dit geldt ook voor die van werknemers.

Endpoint-apparaatbeheer kan automatische updates doorvoeren. Het stelt u ook in staat om bedrijfsgegevens te beschermen zonder inbreuk te maken op de privacy van werknemers.

Neem BYOD op in uw Uitdiensttredingprotocol

Als een medewerker uw bedrijf verlaat, is het belangrijk dat u zijn digitale sporen wist.

Ontvangt de werknemer nog zakelijke e-mail op zijn telefoon? Is er nog toegang tot bedrijfsgegevens? Staan er bedrijfswachtwoorden op hun apparaten?

Zorg ervoor dat dit allemaal bij de uitdiensttreding wordt nagegaan.

Hulp nodig bij het veilig implementeren van BYOD in uw bedrijf? Neem vandaag nog contact met ons op.

Nieuw jasje

Voor u ligt een vernieuwde versie van onze Tech Info. Met een moderne, frisse lay-out en meer nuttige informatie over IT en veiligheid, maar zonder plastic jasje. Want minder gebruik van plastic is iets waar we voor een betere toekomst natuurlijk met z'n allen naar moeten streven.

Daarover gesproken: weet u al wat uw streven voor het nieuwe jaar is? Het is tenslotte al december. Heeft u bijvoorbeeld een beoordeling van uw IT-infrastructuur gedaan? In het artikel op pagina één helpen wij u met uw plannen voor verbetering, een hogere productiviteit en meer winst in 2023 door slimmer gebruik te maken van uw technologie.

Verder leest u hoe u het gebruik van privé apparaten van uw medewerkers in uw bedrijfsnetwerk veiliger kunt maken.

Op naar een nieuw jaar zonder onnodige risico's. Wij wensen u alvast fijne feestdagen toe!



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 voor veilig werken bieden.



Madame Curiestraat 13
2171 TW Sassenheim