TECH INFO

PERIODIEKE UITGAVE VAN TROTS IT

IT tips om uw bedrijf vooruit te helpen!

De put dempen

Bijna wekelijks lees je wel iets over een cyberaanval, hack, datalek, praktijken rond phishing e-mails of andere zaken, die bedrijven stilleggen of grote schade aanbrengen. Wereldwijd, maar ook in ons eigen land. Misschien bent u sceptisch over dit onderwerp en denkt u dat het voor een bedrjf als dat van u niet zo'n vaart zal lopen. Toch is het belangrijk over deze risico's na te denken. En de manier waarop u ermee omgaat.

Gaat u reageren wanneer de schade al is aangericht of wilt u het risico voor zijn? Bent u reactief of pro-actief in het beschermen van uw bedrijfsnetwerk? Wordt de put gedempt als het kalf verdronken is of zorgt u ervoor dat dat gat allang is gedicht, voordat er iets mee kan gebeuren?
Over dit soort zaken en meer gaat deze nieuwste Trots IT Tech Info.

Doe er uw voordeel mee!

December 2020

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.

Het maken van deze ene fout met uw computernetwerk kan leiden tot faillissement

Hoe gaat u om met netwerkproblemen? Als u net als de meeste MKB'ers bent, wacht u tot er iets kapot of mis gaat voordat u een IT-servicebedrijf aan de lijn krijgt. In eerste instantie is dat logisch. Waarom betalen om iets te repareren als het niet kapot is?

Helaas kan deze manier van denken meer kwaad dan goed doen en heeft het veel bedrijven uitgeschakeld.

Welbeschouwd zijn er twee voornaamste manieren om met netwerkbeveiliging om te gaan:

- **Door reactief te zijn**
- **Door proactief te zijn**

Een van deze kost aanzienlijk meer dan de andere en kan funest zijn voor een bedrijf. U kunt waarschijnlijk raden over welke we het hebben. Wanneer u reactief bent met uw IT-services, waaronder gegevensbeveiliging, betekent dit dat er al iets ergs is gebeurd. Er zijn veel verschillende dingen die uw gegevens en uw bedrijf kunnen schaden, zoals een werknemer die per ongeluk malware op zijn computer downloadt. U kunt getroffen worden door een datalek of een stroompiek die laat in de nacht na een onweersbui optreedt.

Reactief zijn, opent echter in feite de deur voor deze bedreigingen. Het is dé fout waardoor u voorgoed failliet kunt gaan.

Hackers vormen bijvoorbeeld een ENORME bedreiging voor kleine bedrijven. Deze cybercriminelen doen er alles aan om in uw netwerk in te breken en te stelen wat ze maar kunnen bemachtigen of welke schade dan ook aan te richten. Deze mensen kan het niet schelen of hun handelen u buiten bedrijf stelt.

Vervolg op pagina 2

Vervolg van pagina 1

Daarom kunt u niet vertrouwen op een reactieve benadering van uw IT-diensten. Als u dat doet, loopt u bij malware en zelfs natuurrampen en apparatuurstoringen achter de feiten aan.

In het verleden waren IT-servicebedrijven erg reactief. Ze zijn gebouwd op het break-fix-model en dat is precies zoals het klinkt. Een bedrijf wachtte tot er iets kapot of fout ging, voordat het een IT-servicebedrijf belde voor hulp bij het oplossen ervan.

In de jaren negentig en zelfs in de jaren 2000 had het break-fix-model zijn plek en het werkte. Maar toen de technologie verbeterde en het voor zelfs de kleinste bedrijven gemakkelijker werd om vooruitstrevend te blijven, was het break-fix-model niet langer logisch.

Het aantal externe dreigingen is de afgelopen 10 jaar drastisch gestegen. Er zwerven talloze malwareprogramma's rond op internet en hackers werken 24/7 om grote schade aan te richten.

Het is tijd om proactief te worden.

Tegenwoordig kunnen IT-servicebedrijven bedreigingen voorspellen. Ze kunnen aanvallen op hun pad stoppen en uw bedrijf en uw gegevens beschermen. Dit wordt **managed services** genoemd - en het kan uw bedrijf redden.

Wanneer u met een managed services provider werkt, kunt u precies aangeven hoe u proactief wilt zijn. Wilt u dat uw netwerk 24/7 wordt gecontroleerd op bedreigingen? Wilt u dat ze externe toegang hebben tot uw netwerkapparaten, zodat ze u en uw team direct kunnen ondersteunen? Dat kunnen ze allemaal!

Een goed IT-servicebedrijf kan u helpen ervoor te zorgen dat al uw gegevens worden geback-upt en veilig zijn. Ze kunnen ervoor zorgen dat externe bedreigingen worden opgemerkt voordat ze een probleem worden. Ze kunnen ervoor zorgen dat phishing-e-mails u niet blootstellen aan schade. De lijst is eindeloos!

Als u al samenwerkt met een IT-servicebedrijf en deze alleen verouderde break-fix-ondersteuning biedt, is het tijd om te zeggen: "Genoeg!" Eis dat ze proactief worden om uw netwerk te beheren. Wacht niet tot iets stopt met werken om dat telefoontje te plegen. Omdat, zoals veel bedrijven hebben ervaren, wachten op dat telefoongesprek desastreus kan zijn!

GRATIS rapport: 12 onbekende feiten die elke directeur moet weten over data back-up, security en disaster recovery

U ontdekt:

- De enige manier om ZEKER te weten dat uw verloren, beschadigde of gewiste gegevens kunnen worden hersteld – maar minder dan 10% van de bedrijven heeft dit geïmplementeerd
- 7 dingen die u absoluut moet eisen van elke externe back-up leverancier
- Hoe veel back-ups uitvallen en u een vals gevoel van veiligheid geven
- De grootste oorzaak van dataverlies, waar bedrijven niet eens aan denken totdat hun data is gewist

Ontvang vandaag nog uw GRATIS exemplaar via https://www.trotsit.nl/nl/12-onbekende-feiten/

Snelle Weetjes

4 STRATEGIEËN OM DE PRODUCTIVITEIT VAN E-MAIL TE VERBETEREN

Omdat werksituaties nu veel op afstand plaatsvinden, is e-mail nog belangrijker geworden voor communicatie. Zorg er dus voor dat uw e-mailgewoonten goed zijn.

• **Heroverweeg uw onderwerpzin.** Vertel de ontvanger zo veel mogelijk in zo min mogelijk woorden en zorg ervoor dat u de ontvanger laat weten of er actie van zijn kant nodig is.

• **Stel adresseringsregels op.** Het is vervelend om te worden meegekopieerd in een eindeloze reeks e-mailantwoorden. Stel teamregels op over wie op welke e-mails moet letten door de velden “Aan” en “CC” correct te gebruiken.

• **Wees voorzichtig in het gebruik van BCC.** Het blind inkopiëren van mensen in e-mails komt over als achterbaks. Zie er zoveel mogelijk van af. Gebruik het alleen voor bulk-e-mails of als u iemand beleefd uit een reeks wilt halen, die diegene niet langer nodig heeft.

• **Blijf het niet rekken.** Als u iets niet binnen drie of minder e-mails kunt oplossen, wordt het tijd om de telefoon op te pakken. Soms werkt e-mail gewoon niet.

TOP MANIEREN OM NIEUWE OMZETSTROMEN TE IDENTIFICEREN

Er is meer dan één manier om met succes inkomsten te genereren en dit is het moment om de opties te verkennen.

• **Evalueer de markt en bespaar kosten.** Erkennen hoe de behoeften van klanten veranderen, is vooral handig tijdens economische nood. Kosten verlagen is net zo belangrijk, omdat het kiezen van de stroom waarmee u inkomsten wilt genereren en de services die u levert, elkaar moeten kruisen.

• **Blijf zoveel mogelijk trouw aan uzelf.** Wijk niet te ver af van uw core business - concentreer u op wat u goed doet en hoe u waarde toevoegt aan het leven van uw klanten. Er bestaat zoiets als overdiversificatie.

• **Investeer in digitale updates en een divers team.** Technologie kan bedrijven helpen modellen te veranderen om aan de behoeften van de klant te voldoen en inkomsten te genereren. Door dat te koppelen aan een divers personeelsbestand vol verschillende perspectieven, kan dit leiden tot goede ideeën. Business Insider, 24 sep. 2020

4 manieren waarop leiders blinde vlekken kunnen herkennen en overwinnen

Een van de grootste uitdagingen waarmee leiders in hun persoonlijke en professionele ontwikkeling worden geconfronteerd, is het herkennen van blinde vlekken, de onzichtbare obstakels die hen ervan weerhouden hun volledige potentieel te bereiken.

Helaas nemen veel leiders niet de tijd om erachter te komen of ze blinde vlekken hebben. Uit onderzoek van Zenger Folkman bleek dat 30% van de leiders ten minste één grote tekortkoming had waarvan ze niet op de hoogte waren.

Het vinden en oplossen van blinde vlekken is niet voor bangeriken. Het kost veel moeite, durf en discipline om ze te identificeren en corrigeren. Maar het proces doorlopen, helpt de vooruitgang van uzelf en uw bedrijf. Hier zijn vier tips om u te begeleiden.

1. KIJK IN DE SPIEGEL

Voer een zelfbeoordeling uit en categoriseer de u bekende sterke en zwakke punten. Blokkeer tijd in uw agenda en sta geen onderbrekingen toe. Dwing uzelf om lastige vragen te beantwoorden over uw capaciteiten en beperkingen. Schrijf vervolgens de antwoorden op, zodat u beter begrijpt waar u slaagt, waar u tekortschiet en welke stappen u moet nemen om te verbeteren. De inventaris die u tijdens de zelfevaluatie maakt, zal ongelooflijk nuttig zijn wanneer u deze vergelijkt met informatie die uit andere bronnen is verzameld.

2. INZICHT VERWERVEN UIT PERSOONLIJKHEIDSTESTS

Gestandaardiseerde persoonlijkheidstesten zijn een ander hulpmiddel om blinde vlekken op te sporen. Wiley’s DiSC en de Myers-Briggs Type Indicator zijn twee populaire testen die inzicht geven in uw leiderschapsstijl. De meeste van deze beoordelingen zijn gebaseerd op de ‘Big 5’ persoonlijkheidskenmerken: vriendelijkheid, ordelijkheid, extraversie, emotionele stabiliteit en openheid. In vergelijking met uw eigen zelfbeoordeling kunnen de testen meer licht werpen op uw neigingen en voorkeuren in communicatie, besluitvorming en probleemoplossing.

3. VRAAG ANDEREN INPUT OVER UW BLINDE VLEKKEN

Dit is waar het proces moeilijk wordt, maar het is ook de belangrijkste stap die u moet nemen. Vraag verschillende leden van uw team en collega’s om uw sterke en zwakke punten en blinde vlekken op te sommen. Vraag hen manieren tot verbetering aan te bevelen. Als u niet zeker weet of teamleden en collega’s uit angst om kritisch over te komen hun ware gevoelens zullen delen, gebruik dan online tools zoals Google Spreadsheets of Survey Monkey om anonieme feedback te krijgen.

4. MAAK EEN PLAN EN HANDEL ERNAAR

De meest effectieve persoonlijke en professionele ontwikkelingsinitiatieven hebben een plan van aanpak dat de informatie bevat die in de vorige stappen is verzameld en identificeert taken die moeten worden voltooid en mijlpalen die moeten worden bereikt. Het is uw blauwdruk voor succes en helpt u op weg om uw doelen te bereiken. Zorg ervoor dat elk doel SMART is (specifiek, meetbaar, acceptabel, realistisch en tijdgebonden) en dat taken en mijlpalen wekelijks, maandelijks en driemaandelijks worden beoordeeld, zodat u uw voortgang kunt meten. ■

Geoff Smart

Andy Bailey is de oprichter, CEO en hoofdbedrijfscoach bij Petra, een Amerikaanse organisatie die zich toelegt op het helpen van bedrijfseigenaren over de hele wereld om niveaus van succes te bereiken die ze nooit voor mogelijk hadden gehouden. Met de persoonlijke ervaring van het oprichten van een bedrijf t.w.v. 500 miljoen dollar dat hij vervolgens verkocht en verliet, richtte Bailey Petra op om de gaandeweg geleerde principes en praktijken door te geven.

WORD EEN PRO IN VIDEOVERGADEREN VANUIT HUIS

Aan het begin van het jaar waren de meesten van ons er niet klaar voor om thuis videogesprekken te voeren. We waren er gewoon niet goed op ingericht. Nu zijn we praktisch aan het einde van het jaar en hebben we geen excuses meer! Hier zijn vier snelle tips om te veranderen in een professionele videobeller:

1. Geef uw geluid een boost. Een speciale microfoon klinkt veel beter dan de microfoon in uw telefoon of laptop. Het creëren van een optimale geluidsomgeving kan een verschil maken, dus schakel externe luidsprekers uit en houd het gesprek in een rustige omgeving.

2. Pas het beeld aan. Houd uw camera op ooghoogte met een eenvoudige achtergrond. Dit ziet er niet alleen natuurlijker uit, maar het beperkt ook visuele afleidingen en ziet er meteen professioneler uit.

3. Verlicht het. Dit kan snel ingewikkeld worden. U wilt een lichtbron voor u, maar uw computermonitors zijn niet voldoende. U wilt echter geen harde, directe verlichting. Diffuus licht is het beste, maar ringlichten zijn populair onder YouTubers en werken uitstekend voor videogesprekken.

4. Zie er goed uit! Houd eenvoudige overhemden, stropdassen, blouses en andere items in de buurt van de computer, zodat u zich snel kunt omkleden en er professioneel aangekleed uitziet voor een gesprek. Houd het zakelijk casual en vermijd ingewikkelde patronen en felle kleuren die er op de camera ongemakkelijk kunnen uitzien.

Small Business Trends, 28 mei 2020

LATEN UW WERKNEMERS DEZE ACHTERDEUR WAGENWIJD OPEN?

De meeste van uw werknemers hebben thuis draadloze netwerken.

In tegenstelling tot uw zakelijke wifi, missen veel draadloze thuisnetwerken de juiste beveiliging, waardoor er een achterdeur openstaat voor hackers. Wifisignalen worden vaak tot ver buiten de huizen van uw werknemers in de straat uitgezonden. Langsrijdend hacken is tegenwoordig populair onder cybercriminelen.

Hier zijn een paar tips om de wifi-toegangspunten van uw werknemers te beveiligen:

- Gebruik sterkere codering en een complexer wachtwoord.
- Verberg uw draadloze netwerknaam.
- Gebruik een firewall.

Deze beveiligingsmaatregelen zijn niet moeilijk op te zetten. Als u vragen heeft of hulp nodig heeft, zullen wij u graag assisteren om uw medewerkers veilig thuis te laten werken.

HOE WEET IK OF MIJN BEVEILIGINGSCAMERA GEHACKT IS?

Ja, hackers kunnen toegang krijgen tot beveiligingscamera's; loopt die van u risico? Hier zijn drie signalen waar u op moet letten om een gecompromitteerd beveiligingssysteem te herkennen.

U hoort stemmen of andere vreemde geluiden. Sommige hackers houden ervan mensen bang te maken en spreken via het luidsprekersysteem van uw camera. Soms realiseert de hacker zich misschien niet dat het geluid is ingeschakeld. Hoe dan ook, vreemde geluiden kunnen betekenen dat uw camera onmiddellijk moet worden uitgeschakeld.

De camera beweegt. Over het algemeen beweegt de gemiddelde beveiligingscamera niet, maar er zijn veel modellen die op afstand kunnen worden aangepast. Als u een camera ziet bewegen of u vindt hem in een nieuwe positie, controleer hem dan!

Er is ongebruikelijk dataverkeer. Toegang op afstand tot uw camera gebruikt data. Bij veel internetrouters kunt u het datagebruik volgen. Dus als iemand op afstand toegang heeft tot uw camera, moet dat datagebruik worden geregistreerd.

Digital Trends, 1 September 2020

TROTS IT
Madame Curiestraat 13
2171 TW Sassenheim
088-2055888
info@trotsit.nl
www.trotsit.nl
/trotsit/
/company/trots-it