TECH INFO

PERIODIEKE UITGAVE VAN TROTS IT

IT tips om uw bedrijf vooruit te helpen!

Elkaar helpen in Rare tijden

We leven met z'n allen al enkele maanden in rare tijden. Tijden waarin we allemaal zo voorzichtig mogelijk met elkaar omgaan, om onszelf en onze omgeving gezond te houden. Maar ook tijden waarin uw bedrijf ondertussen 'gewoon' moet blijven draaien en uw werknemers, vaak op afstand, ook gewoon en veilig moeten kunnen werken.

In deze eerste editie van onze nieuwsbrief bieden wij u informatie en tips over IT, die uw bedrijf vooruit kunnen helpen. Informatie over de veiligheid van uw bedrijfsdata en systemen, werken op afstand en belangrijke feiten over Cloudcomputing.

Gelukkig is het bij Trots IT 'business as usual'. Wij wensen u, uw bedrijf en uw medewerkers dat ook toe. En als er ook maar iets is, waarbij wij kunnen helpen, aarzel dan niet om contact op te nemen!

Dit is het allerbeste wat u kunt doen om te voorkomen dat cybercriminelen uw netwerk hacken.

Juni 2020

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

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

Er is één ding dat veel kleine bedrijven doen, waardoor ze het risico lopen op een cyberaanval. Ze gaan reactief om met IT-beveiliging. Ze wachten tot er iets ergs gebeurt, voordat ze iets doen.

Helaas leven en werken we in een tijd waarin u niet langer reactief kunt zijn op cyberdreigingen. Vrijwel elk klein bedrijf is verbonden met internet en vertrouwt op een netwerk om te functioneren. Het is de digitale wereld waarin we leven. We hebben te maken met hackers, gegevensverlies, uitval van apparatuur en al het andere dat hoort bij de digitale wereld.

Maar u kunt uw risico verkleinen en voorkomen dat hackers uw netwerk binnendringen door een proactieve benadering van uw cyberbeveiliging en door nauw samen te werken met een ervaren IT-bedrijf, dat weet hoe te navigeren in de digitale wereld van vandaag en alle bedreigingen die daarmee gepaard gaan.

20 tot 25 jaar geleden was reactieve IT-ondersteuning de norm. Als er iets misging, belde u het IT-bedrijf om het te repareren. Maar dingen zijn complexer in 2020. Bedreigingen nemen vele vormen aan en simpelweg reactief zijn werkt niet meer.

Vervolg op pagina 2

Vervolg van pagina 1

Wat houdt proactief zijn met uw IT-ondersteuning precies in?

Het betekent dat uw bedrijf veiliger is en dat u klaar bent om de cyberdreigingen van vandaag aan te gaan. Het betekent dat u werkt met professionals die de tools en middelen hebben om u te beschermen voordat het ergste gebeurt. Het is gewoon logisch.

Werken met een gespecialiseerd IT-bedrijf betekent dat u niet zelf voor uw IT-beveiligingsbehoeften hoeft te zorgen. Als u zoals de meeste kleine bedrijven bent, heeft u niet de middelen om een IT-specialist of een hele IT-afdeling in te huren. Een IT-specialist ter plaatse hebben, kan duur zijn. Omdat er momenteel zo veel vraag naar is, hebben ze een fors loon.

"Werken met een gespecialiseerd IT-bedrijf betekent dat u niet zelf voor uw IT-beveiligingsbehoeften hoeft te zorgen."

Bovendien wilt u geen hiaten in uw ondersteuning. Als uw enige 'IT-man' op vakantie gaat of op een dag niet kan komen, heeft u pech als er iets gebeurt. Wanneer u met een IT-servicebedrijf werkt, is de kans groot dat ze 24/7 ondersteuning aanbieden (veel van de goede doen dat).

Als u 24/7 ondersteuning heeft, wordt het zoveel gemakkelijker om problemen op te vangen voordat ze zich voordoen. Als uw Cloudback-up uitvalt, heeft u ondersteuning. Als hackers proberen uw netwerkbeveiliging te doorbreken, wordt u gewaarschuwd. En al uw software blijft up-to-date met de nieuwste beveiligingspatches. Maar er is meer. U heeft mensen die het beste met u en uw bedrijf voorhebben. Bedenk hoeveel beter u 's nachts zou slapen met dat soort bescherming voor uw bedrijf!

Hier is nog een voordeel van werken met een proactief IT-bedrijf: u kunt uw klanten erover vertellen! U zou er zelfs een verkoopargument van kunnen maken. De consumenten van vandaag zijn meer dan ooit op veiligheid gericht. En met datalekken die elk jaar grote bedrijven treffen, willen uw huidige (en toekomstige) klanten weten dat hun persoonlijke en financiële gegevens veilig zijn.

Wacht niet tot er iets kapot gaat of totdat u bent gehackt voordat u hulp inschakelt. Dat brengt de toekomst van uw bedrijf in gevaar. U moet samenwerken met een IT-servicebedrijf dat klaar en bereid is om proactief uw netwerk te beheren. Een ervaren bedrijf heeft de training, certificering en kennis die nodig is om de hedendaagse cyberdreigingen aan te pakken en tegelijkertijd de behoeften van uw netwerk te beheren.

Pleeg dat telefoontje en laat u niet verrassen door bedreigingen die niet zomaar zullen verdwijnen. Zet kwetsbaarheden om in sterke punten.

Gratis download voor rapport: "Als u cloudcomputing voor uw bedrijf overweegt, doe het niet totdat u dit leest..."

Als u Cloud Computing of Office 365 overweegt te gebruiken om geld te besparen en IT te vereenvoudigen, is het uiterst belangrijk dat u dit speciale rapport krijgt en leest: 5 essentiële feiten die elke ondernemer moet weten voordat hij zijn netwerk naar de Cloud verhuist.

Dit rapport bespreekt in eenvoudige, niet-technische termen de voor- en nadelen van Cloud Computing, gegevensbeveiliging, het kiezen van een Cloudprovider en drie minder bekende feiten die de meeste IT-consultants niet weten of niet zullen vertellen over Cloud Computing, maar uiteindelijk meer problemen zouden kunnen veroorzaken en u meer geld kunnen kosten dan u had verwacht. Zelfs als u nog niet klaar bent om naar de Cloud te gaan, geeft dit rapport u de juiste informatie en vragen om te stellen als het wel zover is.

Ontvang hier uw gratis exemplaar: https://www.trotsit.nl/nl/5-essentiele-feiten/

Snelle Weetjes

4 Manieren om uw bedrijf te laten groeien zonder harder te werken
Stimuleer Resultaten - Volgens het Journal of Economic Psychology houden mensen van geldstimulansen, maar worden ze vaak meer gemotiveerd door beloningen zonder geld. Het kan een week vrij zijn of gratis lunch voor een week. Het enige dat u hoeft te doen, is uw team vertellen welke resultaten u wilt, een creatieve stimulans bieden en de kans is groot dat die resultaten worden behaald!

Geef Prioriteit Aan Tijd - Gebruik de "80/20-regel" als richtlijn. Het staat ook bekend als het Pareto-principe en stelt dat 80% van de effecten afkomstig is van 20% van de oorzaken. Volgens dit principe zou 20% van uw tijd besteed aan taken u 80% van de resultaten moeten opleveren. Als u meer moet doen om resultaten te behalen, herevalueer dan uw aanpak (of neem minder projecten aan).

Evalueer Technologie - Gebruikt u verouderde technologie en software? U zou uw bedrijf kunnen vertragen en de productiviteit kunnen schaden - om nog maar te zwijgen over het feit dat uw bedrijf een ernstig risico loopt op dataverlies of gegevensschending. Kijk wat u nu gebruikt en vergelijk het met wat er op de markt is. Er zijn grote verbeteringen geweest, zelfs in de afgelopen vijf jaar, die de productiviteit enorm kunnen verhogen.

Open Communicatie - Opendeurbeleid is een eind in de goede richting. Heb wekelijkse teamvergaderingen en een chat met heel het bedrijf. Hoe gemakkelijker het is voor individuen en teams om te communiceren, des te gemakkelijker is het voor hen om samen te werken en dat kan de zaken heel soepel laten verlopen. Inc., 13 februari 2020

3 Manieren hoe succesvolle mensen tegenslagen veranderen in succes

1. Ze zeggen: "Kom maar op." Ze willen tegenspoed. Het is wat hen helpt te groeien. Zonder tegenslag of iets dat ons tegenhoudt, kunnen we stagneren. We moeten uitgedaagd worden!

2. Ze nemen gedurfde beslissingen. Succesvolle mensen nemen beslissingen in de wetenschap dat ze veel risico lopen, maar niet het gewenste resultaat zullen krijgen als ze niet doorgaan. En als ze de verkeerde beslissing nemen, zal het een leermoment zijn.

3. Ze omarmen de leerzame ervaring. U kunt niet groeien en succes vinden zonder continu te leren. U moet problemen oplossen en samenwerken met anderen, zodat het gemakkelijker is voor u om u aan te passen als de volgende uitdaging zich aandient.
Business Insider, 13 februari 2020

Cybercriminelen zijn in volle gang in deze gekke tijden- hier leest u hoe u ze kunt stoppen

De afgelopen maanden is vrijwel iedereen gedwongen de prioriteiten te verleggen. Als u net als veel andere ondernemers bent, concentreert u zich intensief op het laten draaien van uw bedrijf en aan te passen aan het 'nieuwe normaal'. U investeert waarschijnlijk zoveel van uw tijd in het proberen uw klanten te behouden en nieuwe cashflow te genereren dat u amper tijd heeft om zelfs maar na te denken over cyberveiligheid.

Het probleem is dat cybercriminelen en hackers weten dat er geen betere tijd is om toe te slaan, dan tijdens een wereldwijde crisis. In feite werken ze waarschijnlijk overuren om nieuwe malware te maken, terwijl de rest van ons probeert te dealen met hoe ons leven op zijn kop is gezet. Terwijl u zo gefocust bent op uw bedrijf, vinden deze cybercriminelen nieuwe manieren om uw IT-netwerk te betreden, zodat ze gegevens en wachtwoorden kunnen stelen, de privé-informatie van uw klanten in gevaar kunnen brengen en zelfs grote sommen losgeld kunnen eisen.

Cybercriminaliteit is al groeiend en zal tegen 2021 naar verwachting 6 miljard euro aan schade veroorzaken! Maar als de geschiedenis zich herhaalt, kun je er zeker van zijn dat hackers nu al op volle kracht bezig zijn. We hebben al gezien hoe de krantenkoppen veranderen van verhalen over COVID-19 tot verhalen over omvangrijke cyberaanvallen op grote en kleine bedrijven.

Hier zijn oplossingen die u kunt implementeren in deze gekke tijden om uw bedrijfsgegevens, geld en productiviteit te helpen beschermen:

1. Wees wantrouwend tegenover inkomende e-mails.
Omdat mensen al een tijdje bang, verward en niet echt gefocust zijn, is dit het perfecte moment voor hackers om e-mails te verzenden met gevaarlijke malware en virussen. U heeft waarschijnlijk een aantal op COVID-19 gerichte e-mails ontvangen. Inspecteer de e-mail altijd zorgvuldig en zorg ervoor dat u de afzender kent. Er zijn al e-mailadressen zogenaamd vanuit gezaghebbende overheidsorganisaties, die wereldwijd spam hebben gepost.

Klik niet op links in de e-mails, tenzij duidelijk is waar ze naartoe gaan. En u mag nooit een bijlage downloaden tenzij u weet wie deze heeft verzonden en wat het is. Communiceer deze beveiligingen aan iedereen in uw team, vooral als ze vanuit huis werken.

2. Zorg ervoor dat uw thuiswerkcomputers veilig zijn.
Een andere reden om in deze tijden een toename van cyberaanvallen te verwachten, is de dramatische toename van het aantal thuiswerkers. Veel te veel werkgevers denken niet na over beveiliging als hun team aan de keukentafel gaat werken. Dat is een gevaarlijk precedent.

Zorg er eerst voor dat uw werknemers hun thuiscomputers of thuisapparaten niet gebruiken tijdens het werk. Zorg er ten tweede voor dat uw thuiscomputers een firewall hebben die is ingeschakeld. Ten slotte zijn uw netwerk en gegevens niet echt veilig, tenzij uw werknemers een virtueel particulier netwerk (VPN) gebruiken. Als u hulp nodig heeft bij het inrichten of verbeteren van uw nieuwe thuiswerkomgeving, dan richten wij dat graag voor uw hele team in. Ons doel is altijd om uw bedrijf te laten floreren met meer cyberveiligheid en superieure technologie die de efficiëntie verbetert.

Vervolg op pagina 4

“Cybercriminaliteit is al groeiend en zal tegen 2021 naar verwachting 6 miljard euro aan schade veroorzaken!”

Vervolg van pagina 3

3. Verbeter uw wachtwoordstrategie.
Tijdens crises als deze kunnen uw wachtwoorden het verschil betekenen tussen uw tijd besteden aan het uitbreiden van uw bedrijf en het proberen terug te halen van financiën en privégegevens die zijn gehackt. Evalueer uw wachtwoorden opnieuw en vraag uw team om sterkere wachtwoorden te maken.

Hoewel het erg handig is om uw wachtwoorden op te slaan in uw webbrowser, vermindert het ook uw veiligheid. Omdat webbrowsers eenvoudigweg hun eigen wachtwoord of pincode nodig hebben om toegang te krijgen tot opgeslagen wachtwoorden, kan een ervaren hacker deze hindernis omzeilen. Zodra ze toegang hebben tot uw opgeslagen wachtwoorden, kunnen ze zoveel stelen als ze willen: creditcardgegevens, privégegevens van klanten en meer!
In plaats daarvan zou u een wachtwoordbeheerder moeten overwegen om al uw wachtwoorden op één plaats te bewaren. Deze wachtwoordbeheerders bieden robuuste beveiliging.

U, uw team en uw gezin hebben op dit moment genoeg om u bezig te houden. U hoeft niet nog meer problemen op uw hals te halen, door uw computer en netwerkbeveiliging tijdens deze tijden te laten glijden.

Hoewel deze coronavirus-angst talloze bedrijven negatief heeft beïnvloed, kunnen we met trots zeggen dat we open zijn en onze klanten voortdurend van dienst zijn. Als u aanvullend beveiligingsadvies nodig heeft of als u een consult wilt hebben om te bespreken hoe u uw gegevens veilig kunt houden of hoe we u kunnen helpen effectiever te werken, neem dan vandaag nog contact met ons op.

In deze editie:

Het allerbeste wat u kunt doen, om te voorkomen dat cybercriminelen uw netwerk hacken | 1

Gratis rapport over Cloudcomputing | 2

Snelle Weetjes | 3

Cybercriminelen zijn in volle gang | 3

Wat klanten over ons zeggen

“Trots IT houdt onze systemen op afstand in de gaten en up-to-date. Zij komen gemaakte toezeggingen en afspraken daadwerkelijk na en houden ons altijd op de hoogte van ondernomen acties.”

“Bij Trots IT onderhouden ze onze IT middelen en werken ze proactief. Hun deskundig personeel monitort en waakt voortdurend over onze IT-omgeving om te voorkomen dat verstoringen escaleren.”

“Het grote voordeel van samenwerken met Trots IT voor onze telefonie, infrastructuur en computers is de uitgebreide kennis van zaken die zij bezitten. Wij kunnen altijd met onze vragen en problemen op dat gebied bij ze terecht en krijgen steevast een bevredigend en oplossingsgericht antwoord.”

“Ze staan dichtbij je bedrijf en bieden een snelle respons. Juist met dat persoonlijke en die betrokkenheid steekt Trots IT met kop en schouders uit boven de vorige IT-dienstverleners.”

Colofon

Dit is een gratis periodieke uitgave

TROTS IT

Madame Curiestraat 13
2171 TW Sassenheim
088-2055888
www.trotsit.nl
info@trotsit.nl

Juni 2020