TECH INFO

PERIODIEKE UITGAVE VAN TROTS IT

IT tips om uw bedrijf vooruit te helpen!

Revolutie

U heeft het misschien niet zo in de gaten, maar er is in de wereld van IT al een tijdje een stille revolutie gaande. Een nieuwe benadering van hoe we omgaan met het beschermen van bedrijfsgegevens en het beheren van inloggegevens.

Deze verandering in Identity Management, want zo wordt het ook wel genoemd, heeft betrekking op de manier waarop medewerkers toegang krijgen tot het bedrijfsnetwerk. De manier van inloggen, het zogenaamde authenticatieproces, heeft namelijk invloed op de veiligheid van het bedrijfsnetwerk en de gevoelige data van een organisatie.

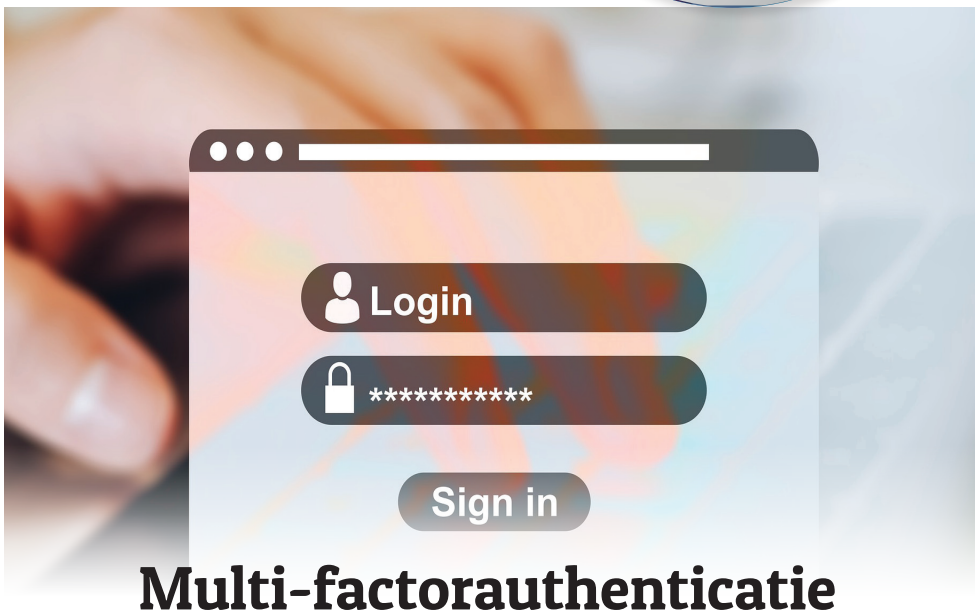
En Trots IT zou Trots IT niet zijn, als we daarin niet voorop zouden lopen. Onze nieuwste tool GateKeeper is namelijk een van de meest veilige manieren van multi-factorauthenticatie gebleken. En de handigste, met zijn wachtwoordloze en contactloze authenticatie.

Deze editie van onze Tech Info staat voor een groot deel in het teken van dit revolutionaire authenticatiesysteem. Doe er uw voordeel mee!

Augustus 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.



Multi-factorauthenticatie Welke Vorm Is Het Veiligst en Welke Het Handigst?

Het stelen van inloggegevens is big business geworden. Het heeft inmiddels een recordhoogte bereikt en is verantwoordelijk voor meer gegevensinbreuken dan elke andere cybercrimevorm.

Nu gegevens en bedrijfsprocessen grotendeels cloudgebaseerd zijn, is het wachtwoord van een gebruiker de snelste en gemakkelijkste sleutel tot het uitvoeren van veel verschillende soorten gevaarlijke activiteiten.

Ingelogd als gebruiker (vooral als ze de beheerdersrechten hebben), kan een crimineel phishing-e-mails van uw bedrijfsaccount naar uw personeel en klanten sturen. De hacker kan ook uw cloudgegevens met ransomware infecteren en duizenden bitcoins eisen om het terug te geven.

Hoe beschermt u uw online accounts, gegevens en bedrijfsvoering tegen al deze dreigingen? Een van de beste manieren is met **multi-factorauthenticatie (MFA).**

Multi-factorauthenticatie vormt een aanzienlijke barrière voor cybercriminelen, zelfs als ze geldige gebruikersgegevens hebben om in te loggen. Dit komt omdat ze in principe geen toegang hebben tot het apparaat dat de MFA-code ontvangt, die nodig is om het authenticatieproces te voltooien.

Wat zijn de drie belangrijkste manieren van MFA?

Wanneer u multi-factor authenticatie in uw bedrijf implementeert, is het belangrijk om de drie belangrijkste methoden van MFA met elkaar te vergelijken en niet gewoon aan te nemen dat alle methoden hetzelfde zijn. Er zijn belangrijke verschillen die sommige niet alleen veiliger maken dan andere maar vooral handiger en beter passend bij uw bedrijfsactiviteiten.

Deze drie belangrijkste manieren van MFA zijn:

Sms-gebaseerd

De meest bekende vorm van MFA is gebaseerd op sms. Deze gebruikt sms-berichten om de gebruiker te authentiseren.

Gebruikers voeren meestal hun mobiele nummer in bij het instellen van deze vorm van MFA.

Vervolg op pagina 2

Vervolg van pagina 1

Wanneer ze vervolgens inloggen op hun account, ontvangen ze een sms met een code die binnen een bepaalde tijd moet worden ingevoerd.

Code in app op smartphone

Een andere manier van multi-factorauthenticatie gebruikt een speciale app om de code te verzenden. De gebruiker genereert bij het inloggen nog steeds de MFA-code, maar in plaats van de code via sms te ontvangen, wordt deze ontvangen via de app.

Dit gebeurt meestal via een pushmelding en kan in veel gevallen worden gebruikt met een mobiele app of desktop-app.

Beveiligingssleutel

De derde belangrijkste manier van MFA omvat het gebruik van een afzonderlijke beveiligingssleutel die u in een pc of laptop moet plaatsen om de aanmelding te verifiëren. De sleutel zelf wordt tegelijk met het instellen van de MFA-oplossing aangeschaft, en is hetgene wat de authenticatiecode ontvangt en automatisch implementeert.

Wat zijn nou eigenlijk de verschillen tussen deze drie methoden?

Handigste vorm van MFA?

Gebruikers hebben vaak het gevoel dat MFA hen tijdens het werk vertraagt. Dit kan erger zijn als ze een nieuwe app moeten leren gebruiken of een beveiligingssleutel niet moeten vergeten (wat als ze die sleutel kwijtraken?).

Dit gebruikersongemak kan ertoe leiden dat cloudaccounts van bedrijven niet goed beschermd zijn omdat de multi-factorauthenticatie niet wordt gebruikt.

Als u te maken krijgt met deze weerstand en op zoek bent naar de handigste vorm van MFA, dan lijkt dit de op sms gebaseerde MFA zijn.

De meeste mensen zijn al gewend aan het ontvangen van sms-berichten op hun telefoon, dus er hoeft geen nieuwe interface worden geleerd of app geïnstalleerd. Het nadeel hiervan is wel, dat afhankelijk van de gemaakte instellingen de computer niet op slot gaat maar voor iedereen toegankelijk blijft of na elke inactiviteit een nieuwe code nodig heeft.

Veiligste vorm van MFA?

Als uw bedrijf gevoelige gegevens in een cloudplatform verwerkt, zoals bijvoorbeeld uw online boekhoudoplossing, kan het in uw eigen belang zijn om bij de keuze voor multi-factorauthenticatie voor veiligheid te gaan.

De veiligste vorm van MFA is de **beveiligingssleutel.**

Bij de varianten met een code in sms of app zouden uw accounts in geval van verlies of diefstal van uw mobiele telefoon voor anderen toegankelijk kunnen zijn en dus in gevaar komen. Omdat de beveiligingssleutel een afzonderlijk apparaatje is dat direct aan uw pc of laptop wordt gekoppeld en zich uitsluitend daarop identificeert, is er bij dit scenario geen risico.

De sms-gebaseerde versie is eigenlijk het minst veilig omdat er tegenwoordig malware bestaat die een simkaart kan klonen, waardoor een hacker die MFA-tekstberichten kan ontvangen.

In een onderzoek van Google werd gekeken naar de effectiviteit van deze drie manieren van MFA voor het blokkeren van drie verschillende soorten aanvallen: geautomatiseerde bots, phishing en gerichte aanvallen. De beveiligingssleutel was in alle gevallen het veiligst.

Percentages van geblokkeerde aanvallen:

- Op SMS gebaseerd: tussen de 76 en 100%
- Op app gebaseerd: tussen de 90 en 100%
- Beveiligingssleutel: 100% voor alle drie de aanvaltypes

GateKeeper authenticatiesysteem

In het kader van veiligheid is multi-factorauthenticatie met een beveiligingssleutel dus de beste optie. Het goede nieuws is dat er tegenwoordig ook een handige manier van deze optie beschikbaar is. Een manier waarbij het onthouden en typen van wachtwoorden niet meer nodig is en uw medewerker altijd direct toegang tot zijn computer heeft. Het GateKeeper wachtwoordloze authenticatiesysteem is een revolutionaire nieuwe manier voor altijd volledig automatische, contactloze en veilige toegang zonder wachtwoorden.

Op zoek naar hulp voor het instellen van MFA in uw bedrijf?

Multi-factor authenticatie is een onmisbare oplossing in het huidige dreigingsklimaat. Wij helpen u graag om deze manier van identity management in uw bedrijf te implementeren en zo uw cloudomgeving beter te beveiligen.

Kijk op www.trotsit.nl/gatekeeper voor meer informatie of bel ons via 088-2055888 voor een vrijblijvende afspraak.

TROTS IT IN HET NIEUWS

Soms bestaat het leven uit toevalligheden, waarbij iets of iemand precies op het juiste moment op je pad komt.

Dat gebeurde recent ook bij Trots IT. Toen wij aanwezig waren op een netwerkevent bij Provalu, het regionale verbindingscentrum voor werk, ontwikkeling en re-integratie, waar werkzoekenden met afstand tot de arbeidsmarkt zich op dat moment voorstelden. Ook Maryam, een hooggekwalificeerde IT-er met internationale werkervaring en kennis, stelde zich als werkzoekende voor.

Die internationale kennis en ervaring zet zij dankzij de bemiddeling van Provalu inmiddels in voor de klanten van Trots IT. Want Maryam bleek zo'n goede match met ons en onze werkwijze te zijn, dat wij haar graag een kans gaven als nieuw lid van het Trots IT team. Voor Maryam een mooie uitdaging en voor Trots IT een stapje verder in sociaal maatschappelijk verantwoord ondernemerschap.

Voor het complete verhaal over de totstandkoming van deze samenwerking verwijzen wij u graag naar het nieuwsartikel op de website van Provalu.

HOE U MEER KANSEN CREËERT

Welbeschouwd bestaat het hele leven uit perspectief. Elke activiteit, baan en situatie heeft meestal meerdere invalshoeken, afhankelijk van hoe u het bekijkt. Door ons perspectief in ons zakelijke en persoonlijke leven te veranderen, ontstaat er een positieve mindset die ons openstelt voor een overvloed aan nieuwe kansen.

Achter mijn huis staat een kleine rotswand. Normaal gesproken zou ik geen seconde nadenken over dit enorme stuk steen dat zich achter in mijn tuin bevindt, omdat hij levenloos is. Het is tenslotte maar een steen, toch? Maar naarmate ik het vaker observeerde, veranderde mijn perspectief volledig.

Want hoewel de rots zelf misschien levenloos is, wemelt hij in feite van het leven. Er zijn prachtig gekleurde hagedissen die in de spleten van de rots leven en ik zag er zelfs een grote zwarte rattenslang. Toen ik erover nadacht, realiseerde ik me dat dit rotsblok zijn eigen ecosysteem in stand houdt.

Door simpelweg even de tijd te nemen om uw eigen vooroordelen los te laten en de moeite nemen om te observeren, zult u leven en kansen vinden in iets wat u eerder misschien over het hoofd hebt gezien. Maar je perspectief veranderen is makkelijker gezegd dan gedaan.

Om uw perspectief te veranderen, moet u misschien een beetje de diepte in. U zult moeten onderzoeken waarom u de dingen ziet zoals u ze ziet. Het kan nodig zijn om met anderen in gesprek te gaan en hun perspectieven te bekijken om een idee te krijgen hoe anderen denken. En ten slotte moet u uw eigen perspectief opnieuw vormgeven, zodat u kunt groeien en nieuwe kansen kunt vinden.

Verdiep u meer in uzelf en concentreer u echt op dat waarop u wilt focussen. Dan zult u zoveel meer zien. U zult snel ontdekken dat de mogelijkheden eindeloos zijn.

Mike Michalowicz heeft altijd geloofd dat hij de formule voor succes had en heeft dat op meerdere momenten bewezen. Hij is de bedenker van ***Profit First****, dat wereldwijd door honderdduizenden bedrijven wordt gebruikt om winst te maken. Hij is de auteur van meerdere boeken, waaronder* ***Get Different*** *en* ***The Toilet Paper Entrepreneur****. Mike is voormalig MKB-columnist voor* ***The Wall Street Journal*** *en was een deskundige in bedrijf make-overs voor de Amerikaanse nieuwszender MSNBC. Mike leidt momenteel twee nieuwe miljoenenbedrijven terwijl hij zijn nieuwste onderzoek test. Hij is ook een veelgevraagd keynote spreker over innovatieve ondernemersonderwerpen.*

3 SOORTEN TECHNOLOGIE DIE ELK BEDRIJF NODIG HEEFT

In de afgelopen 20 jaar heeft de technologie zich snel ontwikkeld tot een niveau dat voorheen alleen binnen de grenzen van onze verbeelding bestonden. Of u nu een ondernemer bent die een nieuw bedrijf start of een ervaren bedrijfseigenaar, er zijn veel technologische snufjes die u in uw bedrijf kunt integreren om betere resultaten te behalen.

Digitale marketingtools hebben het afgelopen decennium enkele van de grootste ontwikkelingen doorgemaakt. Om de concurrentie voor te blijven, moet u een informatieve en zinvolle aanwezigheid op sociale media hebben die overeenkomt met uw website en andere digitale campagnes. U moet ook investeren in cloudtechnologie, omdat uw bedrijf hierdoor een enorme ontwikkeling kan doormaken in de manier waarop u informatie deelt. Als uw bedrijf met klanten te maken heeft, kan het bijzonder nuttig zijn om met software voor klantrelatiebeheer aan de slag te gaan. Verschillende onderzoeken hebben een direct verband aangetoond tussen het gebruik van CRM-systemen en positieve klantenbinding.

4 MANIEREN WAAROP BEDRIJVEN KUNNEN VERGROENEN

Er is een hernieuwde aandacht voor hoe bedrijven omgaan met het milieu. Er zijn veel consumenten die liever zaken doen met bedrijven die milieuvriendelijk zijn. Hoewel het fijn is om zo nieuwe klanten aan te trekken, is uw bedrijf op weg helpen naar een groenere en schonere toekomst de beste manier om milieubewust te blijven. Weet u niet waar u moet beginnen? Probeer deze vier eenvoudige methoden voor een groenere werkomgeving.

- Vermijd het gebruik van papier en ga waar mogelijk digitaal.
- Laat – indien mogelijk - uw medewerkers thuiswerken om de CO2-uitstoot te helpen elimineren.
- Bekijk de huidige gewoontes in verbruik en afvalbeheer in uw bedrijf en pas het waar nodig aan.
- Werk samen met milieubewuste leveranciers en partners zodat al uw processen zo groen mogelijk zijn.

PAS OP VOOR DEZE 3 ONLINE DREIGINGEN

Als Mkb'er kent u waarschijnlijk enkele van de verschillende methoden die cybercriminelen gebruiken om gevoelige informatie van uw bedrijf te stelen. Maar er zijn enkele nieuwe bedreigingen die tegenwoordig het nieuws halen. In een recent rapport heeft het Amerikaanse softwarebedrijf CyberCatch 20.000 willekeurig geselecteerde Mkb's in de Verenigde Staten beoordeeld op kwetsbaarheden die door cybercriminelen kunnen worden uitgebuit. Ze ontdekten dat 'spoofing', 'clickjacking' en 'sniffing' nieuwe door deze groepen gebruikte methoden zijn. Methoden die ook bij bedrijven in Europa worden gezien. Maar wat betekenen deze termen eigenlijk?

- Spoofing vindt plaats wanneer een cybercrimineel een vals IP-adres gebruikt om zich voor te doen als iemand die toegang heeft tot het besloten systeem van het bedrijf.
- Clickjacking doet zich voor wanneer een gebruiker op iets klikt dat onschuldig lijkt, maar in werkelijkheid onbetrouwbaar en schadelijk is.
- Sniffing gebeurt wanneer hackers het netwerkverkeer onderscheppen om toegang te krijgen tot niet-versleutelde gegevens.

Om uw bedrijf veilig te houden is het belangrijk om op de hoogte te blijven van alle nieuwe methoden die door cybercriminelen worden gebruikt. Meld u via www.trotsit.nl/cyber-security-tip-van-de-week aan voor onze wekelijkse makkelijk leesbare tips. Zo blijft u ze altijd een stapje voor.

"WAS HET DIE COMPUTER DAAR BENEDEN, WAAR JE PROBLEMEN MEE HAD?"

TROTS IT

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

www.trotsit.nl
/trotsit/
/company/trots-it