10 SEPTEMBER 2021

INVESTEER IN HET VOORKOMEN VAN DIGITALE AANVALLEN IN PLAATS VAN HET VERHELPEN!

www.unitIT.nl

unitit solutions

INLEIDING

We horen het overal: "**Cybersecurity**" maar hoe voorkomen we nou zo'n digitale aanval? Bescherm computers, servers, mobiele apparaten, netwerken en verklein het risico op digitaal gevaar. Door middel van dit whitepaper geven wij u nieuwe inzichten over het cybersecurity beleid. Hoe kunt u zo'n beleid invoeren in uw organisatie? Hoe kunt u uw gegevens beveiligen? U leest het hier.

DIGITALISERING

De wereld wordt steeds digitaler en innovatiever. Vaak biedt dit een hoop voordelen, waaronder het makkelijker uitvoeren van bedrijfsprocessen en het kunnen inspelen op de verwachtingen van klanten, werknemers en partners. Het is belangrijk dat uw organisatie de nieuwe technologieën en ontwikkelingen bijhoudt. Maar nog belangrijker is om dit op een veilige manier te doen! Hoe u dit doet, leggen wij u graag uit.

VEILIGHEID

Digitale veiligheid is van levensbelang voor uw organisatie en heeft betrekking op de continuïteit en zelfs de omzet van uw bedrijf. Heeft u weleens stilgestaan bij de gevolgen van een digitale aanval? Hoeveel omzet verliest u wanneer uw systemen plat liggen terwijl de kosten gewoon doorlopen? Hoe betrouwbaar bent u nog richting uw klanten, leveranciers en medewerkers wanneer hun gegevens in handen komen van criminelen? U moet hier niet aan denken! Daarom is digitale veiligheid belangrijk voor uw organisatie. De beste verdedigingstechniek tegen digitale dreigingen is een gedegen beveiligingsbeleid. Welke afspraken heeft u met uw ICT-partner over het voorkomen van aanvallen? In deze whitepaper vertellen wij u over een gedegen beveiligingsbeleid en de UnitIT-aanpak!

VIER REDENEN WAAROM U VANDAAG NOG MOET INVESTEREN IN DIGITALE VEILIGHEID

1. IEDEREEN LOOPT GEVAAR, OOK U!

"Dit overkomt mij toch niet?!" Wij horen dit vaak maar ook uw organisatie loopt gevaar. Criminelen kijken niet of uw organisatie interessant genoeg is, ze schieten met hagel en kijken waar ze naar binnen kunnen. Aanvallen zijn geautomatiseerd en iedereen is een potentieel doelwit. Simpele maatregelen zoals een goede virusscanner, systemen up-to-date houden, sterke wachtwoorden en het maken en controleren van back-ups verkleinen de kans op een digitale aanval aanzienlijk.

2. BEN BEWUST VAN DE IMPACT!

De impact van een digitale aanval wordt zwaar onderschat. De schade gaat veel verder dan een geldbedrag betalen. Hoeveel omzet loopt u mis zodra u niet meer kunt e-mailen, bellen of bestanden kwijt bent? U kunt uw klanten niet meer helpen, bestellingen kunnen de deur niet uit en uw medewerkers zitten ook stil omdat zij niet meer op hun computer kunnen werken en uw bedrijf heeft een hoop imagoschade. Vertrouwen uw klanten u nog wanneer hun gegevens door u op straat liggen?

3. VOORKOM DAT U NIET MEER KUNT WERKEN!

U bent trots op uw organisatie, u hebt jaren gebouwd aan uw bedrijf en in een klap kunt u niet meer geautomatiseerd werken! Neem maatregelen om dit te voorkomen! Zorg ervoor dat u back-ups maakt en deze ook test en controleert. Een back-up is uw laatste redmiddel bij hacks.

4. CYBERSECURITY HOORT BIJ DE STRATEGIE VAN UW BEDRIJF!

Digitalisering is enorm toegenomen in de afgelopen jaren en zal alleen maar verder toenemen. Dit biedt een hoop kansen maar helaas zijn er ook risico's. Wanneer u niet de juiste maatregelen treft, wordt u een stuk kwetsbaarder en gemakkelijker slachtoffer van digitale aanvallen. Cybersecurity is geen bijzaak, maar vormt een belangrijk onderdeel in uw bedrijfsstrategie!

Benieuwd naar de mogelijkheden? **Klik hier**!

DE UNITIT AANPAK

UnitIT helpt uw organisatie, op basis van een risico gebaseerde aanpak, met een optimale informatiebeveiliging. Onze beveiligingsdiensten sluiten naadloos aan op de diensten die uw huidige ICT partner bieden. Voordat wij beginnen is het voor ons belangrijk om uw organisatie goed te leren kennen. Wij kijken zowel naar uw ICT-systemen, de processen en natuurlijk uw medewerkers. Een perfecte harmonie tussen mens en machine is belangrijk voor een goed cybersecurity beleid. Wanneer we uw processen en risicogebieden in kaart hebben komen we met oplossingen. Betaalbare oplossingen die aansluiten op uw organisatie, zodat u zeker weet waar u in investeert.

HANDVATEN

Om een gedegen cybersecurity plan te bieden voor uw organisatie bestaat de UnitIT aanpak uit vijf handvaten...

1. KENNISMAKEN

Voordat wij een organisatie kunnen voorzien van advies is het belangrijk om kennis te maken. Kennis maken met elkaar en weten wat er speelt binnen uw organisatie. Welke systemen er draaien, welke datastromen zijn er, is uw personeel zich bewust van hun rol in cybersecurity en welke processen hanteert u? Deze vragen krijgen wij inzichtelijk dankzij onze Security Scan. De UnitIT Security Scan toont de status van de beveiliging van uw ICT systemen. Onze scan rapporteert, per apparaat, eventuele kwetsbaarheden en tekortkomingen. U ontvangt een rapportage waarin in duidelijke en begrijpelijke taal wordt uitgelegd welke risico's er zijn, hoe kritiek deze zijn en hoe deze opgelost kunnen worden. Met dit managementrapport heeft u een helder beeld van de eventuele risico's en kunt u met uw huidige ICT partner in gesprek gaan om de eventuele oplossing te implementeren. Indien gewenst kunnen wij hierin ook kunnen adviseren.

2. BESCHERMEN

Door de inzet van de juiste technologie, gecombineerd met getraind en bewust zijnd personeel en goede procedures, worden incidenten voorkomen. Dit is altijd een op maat gemaakt advies. waarbij de volgende punten worden uitgelicht.

Toegangsbeleid

Een goed toegangsbeleid beperkt de toegangsrechten van eigen medewerkers. Geef hen alleen toegang tot de systemen die nodig zijn om de werkzaamheden uit te voeren. Door dit rollen- of functiegebaseerd te maken is dit eenvoudig in te stellen zodat wanneer een medewerker verandert van functie of onverhoopt uw organisatie verlaat de rechten snel worden aangepast of afgenomen. Zorg voor duidelijke documentatie zodat u de toegang in kaart heeft.

Wachtwoordbeleid en Multi-Factor authenticatie (MFA)

Zorg voor een sterk wachtwoordbeleid. Dit is eenvoudig technisch af te dwingen. Met alleen een inlognaam en wachtwoord bent u niet veilig! Zorg dat multi-factor authenticatie actief is.

Data Encryptie

Data encryptie is de conversie van leesbare data naar gecodeerde data. Het is de eenvoudigste manier om te voorkomen dat informatie van een computersysteem, na diefstal, door buitenstaanders kan worden gelezen.

Security Awareness

Meer dan 70% van alle informatiebeveiliging incidenten wordt veroorzaakt door menselijke fouten. Mensen klikken op links in phishingmails en delen, bewust of onbewust, informatie met ongeautoriseerde personen. Medewerkers zijn zich vaak niet bewust van de belangrijke rol die zij vervullen binnen de informatiebeveiliging van hun organisatie. Door het creëren van Security Awareness zullen medewerkers de sterkste schakel vormen en functioneren als ‘human firewall’. Meer informatie treft u hier.

2. BESCHERMEN

Antivirus

Een antivirus is een programma dat uw computer, laptop, tablet, telefoon of ander apparaat beschermt tegen malware. Antivirussoftware, ook wel een virusscanner genoemd, identificeert virussen op uw computer om die vervolgens te stoppen en verwijderen. In de loop der jaren is malware in al zijn vormen steeds slimmer en diverser geworden. De bedrijven die antivirussoftware maken, konden daarbij natuurlijk niet achterblijven. Daarom zijn virusscanners vandaag de dag erg gecompliceerde programma's die op verschillende niveaus en manieren werkzaam zijn. In het volgende onderdeel 'detecteren' vertellen we hier meer over.

Updates

Door uw apparaten te updaten werkt u de (systeem)software en apps bij naar de nieuwste versie waardoor eventuele kwetsbaarheden zijn opgelost, een virus maakt namelijk gebruik van kwetsbaarheden in oudere versies van programma's. Ook draaien de programma's beter omdat updates ook bedoeld zijn om de functionaliteit doorlopend te verbeteren. Steeds meer bedrijven hebben een geautomatiseerd update beleid waardoor ze geen updates meer missen. In het volgende onderdeel vertellen wij hoe u makkelijk zo'n beleid binnen uw organisatie invoert.

3. DETECTEREN

Naast preventieve maatregelen is het ook belangrijk om realtime naar uw data te kijken zodat er snel en doeltreffend gereageerd wordt op bepaalde situaties. UnitIT biedt hiervoor werkplekbeheer. Dankzij onze monitoringtool wordt uw apparatuur 24/7 gecheckt, hierdoor kunnen wij de meeste storingen kunnen voorkomen in plaats van verhelpen. Uw updates worden geautomatiseerd, waardoor u beschikt over de laatste versies van uw programmatuur en zal uw computer niet midden op de werkdag ineens updates gaan installeren. Om uw veiligheid te garanderen draait er continu een proactief antivirus programma en wordt er gescand op ransomware. Mocht u onverhoopt toch slachtoffer worden van een ransomware aanval, wordt het betreffende apparaat direct van het netwerk gehaald waardoor het virus zich niet verder kan verspreiden.

4. REAGEREN

Wanneer voorgaande handvaten goed zijn ingericht, is het mogelijk om incidenten te voorkomen of om snel en doeltreffend te reageren wanneer een incident zich onverhoopts voordoet. Voor de diverse scenario's dienen de juiste maatregelen en procedures beschikbaar te zijn.

Security beheer is de bescherming van systemen, netwerken en programma's tegen digitale aanvallen. Zulke digitale aanvallen kunnen gericht zijn op het stelen, openen, veranderen of vernietigen van gevoelige informatie, op het afpersen van gebruikers of het verstoren van normale bedrijfsprocessen. Het implementeren van een effectief ICT systeembeheer is een complexe uitdaging, zowel technisch als organisatorisch. Temeer omdat de ontwikkelingen en innovaties zich aan de zijde van de kwaadwillende in een hoog tempo opvolgen.

Door onze oplossingen te combineren op het gebied van organisatie, techniek en juridisch kunnen wij, samen met u, een zeer hoog IT beveiligingsniveau realiseren en onderhouden.

5. HERSTELLEN

Ons laatste handvat gaat over herstellen. Hoewel u met de juiste maatregelen te risico's aanzienlijk verkleint, 100% zekerheid dat er nooit meer wat gebeurt heeft u helaas niet. Echter, met de juiste maatregelen bent u snel weer hersteld van een incident en is binnen no-time de normale bedrijfsvoering weer terug.

De behoefte aan een goede back-up is bij elk bedrijf verschillend, sommige sectoren moeten zelfs aan bepaalde wet- en regelgeving voldoen. Samen bepalen wij de vereisten, adviseren wij u over het te voeren beleid en stellen wij een SLA op.

Onderwerpen die aan bod komen zijn o.a. back-up momenten en frequentie, tijdsduur herstel niveau herstel (ieder bestand, een individuele mailbox, een enkel mailtje of de complete omgeving?), data classificatie, archivering, etc. Meer informatie leest u hier

OVER UNITIT SOLUTIONS B.V.

UnitIT is een meedenkende, probleemoplossende partner die organisaties helpt grip te houden op hun ICT. Hierdoor kunnen deze succesvoller zijn, omdat ze zich optimaal kunnen richten op hun kernactiviteiten, ICT dient immers altijd en overal beschikbaar te zijn.

Onze innovatieve en energievriendelijke oplossingen, ingericht volgens 'best practice' en beheerd door onze gecertificeerde medewerkers (o.a. Microsoft Certified) en beproefde procedures (o.a. ITIL), garanderen een optimaal beveiligde en beschikbare ICT-omgeving.

Onze handelwijze kenmerkt zich door een proactieve houding en het ontzorgen van de klant door verantwoordelijkheid te nemen over uw ICT.

VEILIGHEID BESCHIKBAARHEID PRIVACY

UW CONTINUÏTEIT IS ONZE ZORG!

UnitIT Solutions BV
Joulehof 5-7
4622 RG Bergen op Zoom
(The Netherlands)

Telefoon: +31(0)164 27 55
E-mail: info@unitIT.nl
Website www.unitIT.nl
KvK dossiernr.: 220.39479

Silver Microsoft Partner

Preferred Partner