25 OKTOBER 2021

MINISTERIE:
“BEDRIJVEN ZIJN ONVOLDOENDE BEVEILIGD!”

www.unitIT.nl

unitit solutions

HOE IS CYBERCRIME ZO'N PROBLEEM GEWORDEN?

Cybercrime is een enorm probleem geworden voor bedrijven. Volgens het ministerie van EZK zijn bedrijven nog onvoldoende beveiligd, dagelijks vallen vele bedrijven ten prooi aan malware, ransomware en phishing, de meest voorkomende vormen van cybercriminaliteit. Via e-mail, sms of WhatsApp 'vissen' criminelen naar informatie. De afzender doet zich voor als iemand anders, stelt je vragen en zet je onder druk om op een link te klikken. Een ander veel voorkomend probleem is het gijzelen van computers waarbij de cybercriminelen geld vragen om de computer weer te 'bevrijden' of via valse e-mails internetgebruikers naar een nagebootste website lokken. We denken allemaal: "dát gebeurt mij niet!" maar de cijfers liegen niet, elke dag weer opnieuw...

1. OPMARS VAN DIGITALISERING

Digitalisering blijft in opmars, van thuiswerken tot aan het werken in de Cloud. Ondanks de versoepeling van de COVID-maatregelen waardoor we weer naar kantoor gaan, zullen organisaties meer gaan investeren om thuiswerken te faciliteren. Er wordt verwacht dat 80% van de bedrijven de komende vijf jaar investeert in oplossingen die het thuiswerken ondersteunen. Denk hierbij aan het inrichten van virtuele werkplekken, video vergaderen en het automatiseren van processen. Het beheer en het waarborgen van de veiligheid van bedrijfsgegevens wordt daarom steeds belangrijker want deze zullen niet enkel meer 'binnen' de organisatie blijven maar steeds meer ook vanaf buiten beschikbaar moeten zijn. Security beheer draagt bij aan de optimalisatie van de kwaliteit, doorlooptijden, opbrengst en resultaten. Het is belangrijk dat de data en documenten op een centrale plaats beschikbaar zijn voor alle betrokkenen. De reden waarom 49% van het MKB aangeeft meer te gaan investeren in de Cloud.

2. WAAROM NEEMT NOG NIET IEDER BEDRIJF CYBERCRIME SERIEUS?

Met alle veranderingen van de afgelopen tijd, begrijpen wij maar al te goed dat u niet gelijk denkt aan security beheer. De cijfers wijzen uit dat er in Nederland nog veel te weinig wordt geïnvesteerd in security. Waar ligt dat aan? Een van de belangrijkste

redenen is dat er geen direct zichtbaar resultaat is van de investering in beveiliging. De pers maakt alleen melding van bedrijven met een grote naamsbekendheid terwijl juist de onbekendere MKB-bedrijven het meest worden aangevallen met vaak grote schade en niet zelden ten onder gaan aan deze vorm van criminaliteit. Het MKB lijkt de ernst niet in te zien, heeft vaak blindelings vertrouwen in de cloud of is zich niet bewust dat ze juist wél interessant genoeg zijn voor cybercriminelen. Het is belangrijk dat het MKB inziet dat niet uit te sluiten is dat cybercriminelen al meekijken met de organisatie maar dit nog niet hebben opgemerkt. Wanneer een bedrijf geen professionele ICT-afdeling of gespecialiseerd personeel heeft, zal de ICT-omgeving onvoldoende veilig ingericht zijn.

3. WAAROM MOETEN BEDRIJVEN NU IN ACTIE KOMEN?

Door het massale thuiswerken tijdens de COVID-crisis moesten veel bedrijven ineens meer aandacht besteden aan hun ICT zodat er op afstand 'gewoon' doorgewerkt kon worden. Dit betekende dat de vraag naar professionele ICT-kennis groter werd en dat bedrijven hun ICT-omgeving gingen uitbesteden aan ICT-organisaties. Naast de beschikking over specialistische, professionele kennis bij een ICT-partner, biedt een goed ingerichte en beheerde ICT-omgeving enorme voordelen voor elk bedrijf. Een paar voordelen op een rijtje:

1. De continuïteit van uw bedrijfsprocessen is beter gegarandeerd;
2. Geen last van afwezig personeel (ziekte, vakantie, etc.), uw ICT-partner zorgt, immers voor uw ICT;
3. Het is vaak goedkoper dan iemand in dienst nemen (zeker voor kleinere bedrijven);
4. ICT-organisaties beschikken over gespecialiseerd en gecertificeerd personeel met een brede, hoge, actuele kennis en hebben veel ervaring;
5. Een ICT-organisatie kan ook ondersteuning verlenen buiten kantoortijden;
6. U heeft slechts één aanspreekpunt voor alle ICT-gerelateerde vragen;
7. Uw omgeving wordt door monitoring constant bewaakt en er wordt proactief gehandeld bij incidenten, issues en teruglopende prestaties.

Het uitbesteden van de ICT-omgeving ontzorgt, geeft minder stress en creëert meer tijd om u te focussen op de kernactiviteiten van uw bedrijf. Daarnaast is uw ICT-partner in staat om platformen continu te vernieuwen en te verbeteren. Zo maakt u altijd gebruik van de nieuwste technologieën zonder dat u zelf hoeft te investeren in kennis en apparatuur.

Kortom, het uitbesteden van uw ICT-omgeving brengt veel voordelen met zich mee. Overweegt u om uw ICT-omgeving uit te besteden en wilt u daar meer over weten? Onze specialisten staan voor u klaar. 0164-275533 of **info@unitit.nl**

WELKE VORMEN VAN CYBERCRIME ZIJN ER?

Cybercrime komt voor in vele varianten. Het is belangrijk om de vormen van cybercrime enigszins te kennen zodat u zelf al kunt inspelen op de gevaren. Hieronder een korte opsomming van de verschillende vormen van cybercrime:

VIRUS/MALWARE

Een virus of een malware is een klein programma dat de werking van uw computer verstoort. Een virus kan gegevens op uw computer beschadigen of verwijderen, uw e-mailprogramma gebruiken om zichzelf te verspreiden of zelfs de hele harde schijf wissen. Veel virussen worden per e-mail verspreid en zijn vermomd als onschuldige bijlage, zoals een foto of tekstdocument.

PHISHING

Het per mail 'hengelen' naar informatie door criminelen wordt phishing genoemd. Via de mail (maar ook via de telefoon) lijken betrouwbare instanties zoals bijvoorbeeld een bank te vragen om uw inloggegevens, uw pincode of andere persoonlijke informatie.

RANSOMWARE

Een computervirus dat probeert u geld te laten betalen om van het virus af te komen. Ransomware kaapt uw computer door uw bestanden te blokkeren waardoor ze niet meer toegankelijk zijn. Het virus meldt dat je een geldbedrag moet betalen om van de blokkade af te komen.

CRYPTOJACKING

Een vorm van cybercrime waarbij cybercriminelen geld willen verdienen door cryptogeld in handen te krijgen. Dit doen ze door in te breken op zoveel mogelijk Wifi-netwerken, computers en websites, ook van mensen die niet in cryptogeld handelen.

HELPDESKFRAUDE

Bij deze vorm van oplichting waarbij fraudeurs vaak vanuit landen als India bellen en doen alsof ze helpdeskmedewerkers van grote, bekende bedrijven zijn, zoals Microsoft, Google en Ziggo. Ze zeggen dat uw computer besmet is met virussen of dat uw gehackt bent.

DDOS-AANVALLEN

Distributed denial-of-service (DDoS)-aanvallen hebben als doel een website of internetdienst onbruikbaar te maken door middel van overbelasting van de server. Vaak gaat het om websites van grote commerciële bedrijven, diensten van banken en creditcardmaatschappijen of e-maildiensten. De criminelen achter de aanvallen kunnen veel geld verdienen door hun diensten te verhuren of door bedrijven te chanteren.

HACKING

In het dagelijks taalgebruik verstaan we onder hacken het inbreken in een computersysteem of netwerk. De inbrekers, hackers genoemd, kunnen hiervoor onder meer gebruikmaken van virussen, spyware, phishing en poortscans.

Om grip te houden op de beveiliging, om data maximaal te beschermen en om de continuïteit van uw bedrijf te waarborgen, bieden wij **security beheer**. Security beheer is de bescherming van systemen, netwerken en programma's tegen digitale aanvallen.
Zulke digitale aanvallen kunnen gericht zijn op het openen, veranderen of vernietigen van gevoelige informatie, op het afpersen van gebruikers of het verstoren van normale bedrijfsprocessen. ICT-vraagstukken zijn zeer uiteenlopend en daarom is er brede kennis nodig op meerdere vakgebieden en facetten binnen de ICT. Het kan bovendien veel tijd kosten om het ICT-beheer zelf uit te voeren. Enkele andere nadelen van ICT in eigen beheer zijn:

- Scholing is nodig om het kennisniveau van de ICT-afdeling op peil te houden;
- Eén verantwoordelijke voor de gehele ICT, vergroot de afhankelijkheid;
- Eigen ICT-medewerkers betekent extra personeelskosten;
- Binnen de ICT zijn er heel veel kennisgebieden. Het is onwaarschijnlijk dat één verantwoordelijke kennis van alle gebieden heeft.

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