CYBER SECURITY

VOORKOMEN IS BETER DAN GENEZEN

4CONSULT

CYBER SECURITY VAN 4CONSULT

4Consult is expert op het gebied van cyber security. Om het voor onze partners overzichtelijk te houden, hanteren wij vier verschillende security-pakketten.

In dit document zullen wij deze diensten uitgebreid uitleggen. De vier pakketten zijn:

- DDOS security
- WAN infra security
- Awareness
- Crypto- en ransomware

DDOS SECURITY

Criminaliteit vindt steeds vaker online plaats. Elk jaar zien we het aantal DDOS-aanvallen toenemen in zowel aantallen, grootte als complexiteit.

De kans dat je als bedrijf wordt getroffen is erg groot. Zo groot zelfs, dat het meestal geen kwestie is van of, maar van wanneer, je aan de beurt bent. Wat veel bedrijven niet weten is dat er genoeg te doen is tegen dit soort cyberaanvallen. Niet iedere aanval kan altijd volledig worden gestopt maar door het inzetten van de juiste middelen kan wel de schade aanzienlijk worden beperkt. Veel vaker wordt de aanval zelfs volledig afgeslagen en kun je gewoon doorwerken.

Het doel van een DDOS-aanval is om een bedrijf volledig plat te leggen. Er wordt in de meeste gevallen losgeld geëist waarna de aanval zal stoppen. Helaas heeft het vaak geen enkele zin om te betalen; voor de aanvaller is dit juist een bevestiging dat er “zaken gedaan” kan worden met de betreffende partij. Vaak wordt na de eerste betaling dan ook snel een aanvullend bedrag geëist.

Zonder een goede beveiliging kan je bedrijf in het geval van een DDOS-aanval dagen (of zelfs weken) platliggen. Beter is dus om je vooraf goed voor te bereiden. Er zijn gelukkig diverse middelen voorhanden om ervoor te zorgen dat je afdoende beveiligd bent.

Wat kan 4Consult doen?

Wilt u weten wat de status is van de digitale beveiliging van uw bedrijf? Neem dan contact met ons op en we komen bij u langs voor een onderzoek. Dit onderzoek is erop gericht om binnen uw bedrijf te inventariseren wat er gedaan kan worden om DDOS-aanvallen tegen te gaan. We onderzoeken of het nodig is om extra maatregelen te nemen. Wellicht heeft je bestaande hostingpartij al voldoende maatregelen genomen, maar mocht dit niet het geval zijn dan kunnen we altijd nog verbeteringen doorvoeren.

Het onderzoek wordt in één dag onsite uitgevoerd. Hulp van uw systeembeheerder is hierbij gewenst. Het initiële inventarisatie- en advies-traject kan binnen 8 tot 12 uur plaatsvinden. Afhankelijk van de bevindingen kunnen maatregelen worden genomen. Dit zal gaan op basis van nacalculatie.

Deze dienst is met name geschikt voor bedrijven vanaf 500 werkplekken. Is je orga-nisatie kleiner? Geen enkel probleem! We kunnen je organisatie uiteraard beoordelen en je adviezen geven.

WAN INFRA SECURITY

Hackers worden steeds slimmer en het wordt ook steeds lucratiever om in te breken bij bedrijven. In veel gevallen komen bedrijven er helaas pas na jaren achter dat er hackers actief zijn (geweest) op hun bedrijfsnetwerk.

Vaak is het doel van de aanvaller het verkrijgen van geld (in digitale valuta) door het eisen van losgeld. Maar ook het verkrijgen van informatie is erg interessant voor aanvallers. In het laatste geval merk je vaak niet eens dat er hackers actief zijn op het netwerk.

Als geld verkrijgen het doel is dan ontvang je in veel gevallen een email. Er wordt dan bijvoorbeeld geld geëist omdat anders je gegevens op straat komen of de hackers al je data versleutelen. In steeds meer gevallen wordt zelfs de back-up aangevallen waardoor je ook daar niet meer op kunt terugvallen. Er wordt dan losgeld geëist waarna je een “sleutel” ontvangt. Precieze aantallen zijn niet bekend maar er wordt geschat dat je, ook na betaling, in 50% van de gevallen geen sleutel ontvangt en je dus voorgoed je data kwijt bent. Ook komt het regelmatig voor dat na een eerste betaling nog een tweede of derde betaling wordt geëist.

Er zijn talloze maatregelen denkbaar die de kans op geslaagde digitale aanvallen aanzienlijk verkleinen. Het allerbelangrijkste is dat de toegang tot uw bedrijfsnetwerk vanaf het internet goed is geregeld. Als dit niet goed op orde is dan hebben alle andere maatregelen geen zin meer.

Wat kan 4Consult doen?

Om digitale aanvallen te voorkomen bieden wij een zogenaamde grey-scan aan. Dat houdt in dat wij al wat informatie over je organisatie ontvangen. Denk hierbij o.a. aan ip-nummers. We doen dit zowel van buitenaf (vanaf het internet) als van binnenuit (vanaf het interne netwerk). Hieruit volgt een rapport met adviezen.

De duur van deze scan is afhankelijk van het aantal servers en netwerkapparaten dat binnen de organisatie aanwezig is, maar voor een gemiddeld bedrijf zijn we hier zo’n vier dagen mee bezig. De duur bij kleinere bedrijven (10-200 medewerkers) bedraagt twee tot drie dagen. Hierbij zijn we ongeveer de helft van de tijd onsite aanwezig bij uw organisatie. De hulp van uw systeembeheerder is hierbij gewenst.

Wij komen op een later tijdstip, persoonlijk verslag doen aan het management of de directie van uw organisatie. Het doorvoeren van eventuele verbeteringen doen we op basis van nacalculatie. Aanbevelingen kunnen door de eigen ICT-afdeling worden opgelost maar ook aan ons worden uitbesteed.

AWARENESS

De zwakke plek in de beveiliging van ICT-systemen is helaas maar al te vaak het personeel dat werkt met de systemen. Ongewild zorgen medewerkers voor miljarden euro's aan schade door het klikken op verkeerde linkjes, het openen van besmette bestanden of door het ingaan op verzoeken om mee te kijken door zogenaamde Microsoft-medewerkers.

Onderzoeken tonen aan dat het in 1 op de 10 gevallen lukt om persoonlijke data te verkrijgen door simpelweg te bellen met een bedrijf. Vaak is het nemen van maatregelen op het gebied van cyber security erg complex maar dat geldt niet voor awareness. Goed geïnformeerd personeel dat weet waar ze op moeten letten loopt veel minder risico om slachtoffer te worden van aanvallen. Daarom bieden we bij 4Consult speciale awareness-sessies aan.

Wat kan 4Consult doen?

Deze awareness sessies zijn verhelderend voor alle medewerkers binnen je organisatie. Vooraf proberen we op verschillende manieren informatie te verkrijgen over je bedrijf. We proberen bijvoorbeeld telefonisch een wachtwoord te achterhalen, maar medewerkers zullen ook via SMS, mail of op andere manieren benaderd worden. Uiteraard gaan we nooit verder met het verkrijgen van data dan strikt noodzakelijk en gaan we zeer discreet om met de verkregen data. Wij komen op een later tijdstip persoonlijk verslag doen aan het management of de directie van uw organisatie. Een awareness onderzoek voeren we uit over een periode van 2 tot 3 weken waarbij we ongeveer 10 uur besteden aan het testen en het vastleggen van de resultaten.

Daarnaast verzorgen we awareness trainingen waarbij onderwerpen aan bod komen als: Waarop moet je letten? Wat zou je kunnen doen om ervoor te zorgen dat je beter beschermd bent tegen phishing? Hoe zorg je ervoor dat je personeel meer alert is op dergelijke pogingen om gegevens te verkrijgen? Awareness trainingen geven we ook in blokken van 3 uur met maximaal tien personen. Deze trainingen verzorgen we op locatie of op het kantoor van 4Consult in Ridderkerk-Rijsoord.

CRYPTO- EN RANSOMWARE

Van alle digitale aanvallen is dit wellicht de vervelendste om mee te maken. Er zijn talloze voorbeelden van bedrijven die slachtoffer zijn geworden van crypto- of ransomware aanvallen waarbij het bedrijf de aanval niet “overleeft” en de werkzaamheden heeft moeten staken.

Crypto- en ransomware kan bedrijven letterlijk kapotmaken. Het is daarom goed om even stil te staan bij deze gevaren. Zoals bij alle digitale aanvallen neemt ook het aantal crypto- en ransomware aanvallen jaarlijks toe. Daarnaast worden de aanvallen steeds complexer en worden ook back-ups steeds vaker besmet waardoor het terugzetten van data zo goed als onmogelijk wordt.

Bij crypto- en ransomware gaat het maar om één ding: het verkrijgen van geld in ruil voor een sleutel die ervoor moet zorgen dat je weer de beschikking krijgt over je data. In veel gevallen heeft betalen helaas geen zin en is dit voor de aanvallers juist een trigger voor een nieuwe aanval om meer geld te eisen. Cijfers zijn niet exact bekend maar er wordt geschat dat ongeveer de helft van de gevallen nooit een sleutel wordt afgegeven door de hackers.

Wat kan 4Consult doen?

Crypto- en ransomware kun je op diverse manieren voorkomen. Technisch kun je wel het een en ander doen om aanvallen af te slaan maar de mogelijkheden zijn beperkt. Daarnaast is awareness van uw personeel een belangrijk wapen tegen crypto- en ransomware aanvallen. Immers, ransomware en cryptoware wordt in veel gevallen geactiveerd door het klikken op een verkeerde link of het openen van een gevaarlijk bestand. Ook kunnen we de back-up op de juiste manier voor je inrichten waardoor je altijd nog je gegevens kunt terugzetten. Wij kijken hoe het binnen jouw organisatie is ingericht en we doen aanbevelingen om ervoor te zorgen dat je nooit zonder je data komt te zitten. Je ziet nog te vaak bedrijven die in grote problemen komen omdat dit niet goed geregeld is en dat is tegenwoordig onnodig.

Nodig ons uit en we onderzoeken hoe uw bedrijf ervoor staat en welk risico u loopt in geval van een crypto- of ransomware aanval. We maken een rapport met onze bevindingen en komen deze op een later tijdstip presenteren aan het management en/of de directie van uw organisatie.

TOT SLOT...

Geen enkel bedrijf is hetzelfde en ook een ICT-infrastructuur is niet gestandaardiseerd. Daarom bieden wij onze producten ook op maat aan. Interesse in een op maat gemaakt pakket voor jouw organisatie? Neem dan contact met ons op via 078 – 619 78 10 of stuur even een mailtje naar info@4consult.nl.

4CONSULT

KEEPS YOU GOING!

078 - 619 78 10

info@4consult.nl

www.4consult.nl