Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl.

Hulpgids beveiliging voor het kleinbedrijf (deel 2)

In de vorige uitgave (1) hebben wij een beschrijving gegeven van het belang van het mkb en hoe deze ondernemers begeleid moeten/kunnen worden naar informatie- & ketenveiligheid. Daarbij zijn de eerste vragen en antwoorden gegeven. Ook zijn wij ingegaan op de eerste beschikbare 'tools' en bronnen van informatie.

Het eerste advies betrof de beeldvorming bij de mkb-ondernemer van wat cyberveiligheid inhoudt. Het tweede advies: inventariseer waarom hij/zij zich moet gaan bezighouden met cybersecurity, terwijl het derde advies het gebruik van beschikbare (gratis) gereedschappen aan de orde stelde, zoals onder andere de Cybersecurity Canvas, de CIS-controls en het 5-stappenplan van Patrick Bet-David.

Vincent, een vraag die vrijwel direct rijst is, zijn er ook gereedschappen die mij snel informeren over hoe de vlag bij mij als mkb'er erbij hangt, zonder dat ik eerst zelf binnen mijn bedrijf moet gaan analyseren? Per slot van rekening als mkb'er of als (z)zp 'er, heb ik al zo weinig tijd.

"Dan verwijs ik je naar de **D**igital **T**rust **C**enter (DTC) (2) website en start dan bij de vijf basisprincipes van veilig digitaal ondernemen. Onderaan die DTC-websitepagina

staat de Basisscan Cyberweerbaarheid. Duur: circa vijf minuten. Op basis van 25 stellingen over de vijf basisprincipes word je begeleid bij de status van jouw bedrijfsveiligheid. Let wel: de uitkomst is indicatief!
De vijf basisprincipes van het DTC zijn:
1. inventariseer kwetsbaarheden;
2. kies veilige instellingen;
3. voer updates uit;
4. beperk toegang en
5. voorkom virussen en andere malware.

Het is te adviseren eerst de vijf basisprincipes door te lezen alvorens de scan te starten. Je doorloopt de scan en begrijpt het eindresultaat makkelijker. Elk basisprincipe wordt helder toegelicht en via hyperlinks word je geholpen die analyse handen en voeten te geven. Een vereenvoudigd overzicht van die hyperlinks en geadviseerde stappen:

– inzake kwetsbaarheden:
  – stappenplan risicoanalyse:
    – waaronder ICT-onderdelen inventarisatie;
  – opstellen van een noodplan:
    – leg afspraken vast;
    – stel een uitwijk- en herstelplan op;
  – opstellen van een bellijst:
    – contactgegevens;
– inzake veilige instellingen:
  – IoT-apparaten beveiligen;
  – bedrijfsnetwerk beveiligen;
  – e-mail beveiligingsstandaarden controleren;
  – controleer de veiligheid van het gebruikte wachtwoord;
  – inrichten van een log-informatie systeem;
– inzake updates:
  – een voorbeeld van het opstellen van een patchmanagement-beleid;
  – maak heldere afspraken over welke patches relevant zijn;
  – de controletest of automatisch updaten iets is voor jouw bedrijfsomgeving;
– inzake toegankelijkheid:
  – een link naar een model rechtenmatrix (al of niet met gebruikersrollen);
  – een advies voor realisatie van een in- en uitdiensttredingsbeleid;
– inzake voorkomen van malware en virussen:
  – tips over medewerkersgedrag;
  – antivirusprogramma's en phisingmails.

Vanuit het DTC kun je ook terechtkomen bij hun advies 'Wat te doen bij een cyberincident?', waarom iets zelf uitvinden als het er al is? Daar ook al een overzicht bij wie je terechtkunt na het ondergaan van een cyberincident. Mocht je een IT-specialist in huis hebben of er een inhuren, maar wil je hem ook kunnen volgen/instrueren **inzake het verzamelen van informatie over de daders**, zoek dan het 'Stappenplan voor IT-specialisten' (3) op dat door de politie ter beschikking wordt gesteld."

Er is recentelijk ook vanuit de Kamer van Koophandel een e-mailserie geweest onder de titel: 'Een veiliger bedrijf in 6 stappen'. Hoe sprak je dat aan?
"Deze e-mailserie is gerealiseerd in samenwerking met het DTC en daarom van goede kwaliteit. Het mooie van deze serie is dat ook de collegae mkb-ondernemers aan het woord zijn gekomen. Zij verhaalden van hun cybersecurity-ervaringen en hoe zij geconfronteerd werden met hacks en dergelijke. Het maakt duidelijk dat in de cyberwereld van alles en nog wat kan gebeuren en dat er geen valse schaamte moet zijn om wanneer er iets gebeurd, te handelen en hulp in te roepen. Niets doen, zwijgen of ervan weglopen is geen optie."
OK, er moet gehandeld worden, maar nadat een hack heeft plaatsgevonden of ransomware is geïnstalleerd lijden wij al pijn. Natuurlijk is het beter om op voorhand te acteren. Bekend is back-ups te draaien en na te gaan of je ze ook weer terug kunt zetten. Wat zouden jouw adviezen zijn om jezelf voordien te beschermen?
"Ik wil nu niet direct op alle opties ingaan, maar twee stappen liggen wel erg voor de hand. De eerste betreft het installeren van antivirussoftware en firewalls (gratis zijn redelijke pakketten verkrijgbaar, maar met een overzienbare uitgave kom je al aardig richting semi-professionele pakketten of hardware) en het gebruik van wachtwoorden alsook het beheer daarvan in wachtwoordmanagers (4) — met een open source wachtwoordmanager zoals Bitwarden.com kun je zelfs al gratis aan de slag.

Enkele bekende antivirus- en/of firewallsoftware zijn: AVG, Avast, Avira, Bitdefender, HitmanPro Malwarebytes, Norton, Panda, TotalAV, Webroot SecureAnywhere. Ook kun je met een met advertentie blocker in de browser al tal van virussen gratis voorkomen: uBlock Origin is een gratis extensie, die voor Firefox, Chrome en tal van andere browsers beschikbaar is.

Wat firewalls betreft kan je denken aan: Zyxel, Netgate, Sophos, Cisco, Sonicwall, Fortinet of een gratis open source firewall: vyos.io en pfsense. Mijn lijstje is niet compleet en evenmin in volgorde van kracht of prijsstelling. Laat je door de eigen IT-beheerder/cybersecurity-dienstverlener en/of vertrouwde leverancier voorlichten."

Vincent licht toe:
Het is mijn ervaring dat talrijke cybersecurity-dienstverleners moeite hebben met het vinden van passende oplossingen voor het midden- en kleinbedrijf (mkb). Zelf heb ik jarenlang aan de kant van de securityproviders gewerkt. In die hoedanigheid besefte ik hoe uitdagend het kan zijn om aan te sluiten bij de behoeften van het mkb. De kern van dit probleem schuilt in het onvermogen van serviceproviders om af te stemmen op de pragmatische en zakelijke mentaliteit van mkb-bedrijven. Het is cruciaal om te begrijpen hoe cybersecurity past in zowel de zakelijke als de technische context van de klant, zonder concessies te doen aan het complete cybersecurityplaatje. Helaas slagen veel serviceproviders hier niet in.

Zakelijke context:
De zakelijke omgeving van het mkb verschilt aanzienlijk van die van grotere ondernemingen. In het mkb moet men vlot kunnen schakelen tussen strategische en tactische besluitvorming, aangezien kleinere organisaties doorgaans meer gericht zijn op pragmatisme.

Technische context:
Om succesvol aan te sluiten bij het mkb is het essentieel om snel te kunnen schakelen naar de technische aspecten. Dit is belangrijk omdat techniek in de praktijk de drijvende kracht is waar het meeste werk verzet moet worden.

Compleet cybersecuritybeeld:
Vanwege het beperkte budget en de schaarse middelen binnen het mkb zijn eenvoudige oplossingen vaak aantrekkelijk. Echter, dit kan leiden tot het verlies van het volledige cybersecuritybeeld, wat een cruciaal aspect is voor een effectieve bescherming.

Dank tot zover. Het zal de mkb'er duidelijk zijn geworden dat hij zijn huiswerk vooraf te maken heeft. Kan jij nog andere 'tools' adviseren die de ondernemer op weg naar cybersecurity skillfulness zou kunnen opppakken?
"Jazeker, host je jouw applicaties of een website dan kun je gratis achter de protectie van een Web Application Firewall (WAF) van Cloudflare. Met PingCastle.com kun je gratis jouw Windows **A**ctive **D**irectory (AD) laten scannen op issues en kom je tot praktische verbeteringen. Hardentools is een open source tool waarmee je jouw Windows laptop of PC kunt laten 'hardenen' om zo de meest gevaarlijke features van Windows uit te schakelen (5). Stronghold is een open source tool voor Apple laptops (6). Ook raad ik aan om uBlock Origin te downloaden voor je browser, veel virussen worden namelijk verspreid via advertenties.

Er zijn genoeg tools online te vinden. Toch ziet iedereen steeds vaker dat belangrijke data verstopt zit in SaaS applicaties. Daar zijn vaak geen tools voor. Daarvoor is het van belang dat je een lijstje maakt van alle SaaS applicaties en waarvoor ze gebruikt worden. Vervolgens ga je één voor één de applicaties langs en kijk je of de rechten en users goed staan ingesteld.

In het volgende deel zal ik nog een paar handige APPs aanhalen, maar ik zal ook stilstaan bij wat Windows al aanbiedt in de vorm van automatisch gegenereerde log-informatie databestanden. En dus de vraag aan de ondernemer(s): "Wie van jullie gebruikt al log-rapporten en, zo ja, welke kennen/gebruiken jullie? Laat ook eens weten welke problemen je tegen bent gekomen of welke vragen er verder nog zijn. Benut deze kans."

Referenties

(1) InformatieBeveiliging Magazine, jaargang 23 – 2023 – editie 2, pagina 4 t/m 7
(2) https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen
(3) https://www.politie.nl/binaries/content/assets/politie/algemeen/algemeen/-brochure-stappenplan-cybercrime.pdf
(4) Zie de twee artikelen in InformatieBeveiliging Magazine, jaargang 23 – 2023 – editie 2, pagina 23 ("Password mismanagement" van Lex Borger, Tesorion) en pagina 32 t/m 37 ("De werking en vele functies van wachtwoordmanagers" van Menno Vermeulen, CGI Nederland B.V.)
(5) https://github.com/securitywithoutborders/hardentools
(6) https://github.com/alichtman/stronghold