Cybersecurity: Noodzakelijk

Cybersecurity, ofwel de beveiliging van de ICT-voorzieningen, is een hot item voor zowel ondernemingen als particulieren. Regelmatig melden de media dat er weer een grotere organisatie is gehackt. Maar die aanvallen worden niet alleen uitgevoerd op die grote jongens, ook kleinere ondernemingen moeten op hun hoede zijn voor een digitale inbraak op hun systemen en netwerken.

De inbraken bij de grote bedrijven halen de voorpagina's van de kranten wel, maar met name kleinere bedrijven vormen een makkelijker prooi voor die hackers. Die vallen namelijk in de zogenoemde 'sweet spot' van die internetcriminelen: ze hebben meer digitale waarde-elementen dan particulieren, maar minder beveiligingsmaatregelen dan een grotere organisatie.

Vangnet

De andere reden waarom mkb-bedrijven zulke aantrekkelijke doelen zijn, is omdat hackers weten dat die wat soepeler omgaan met beveiliging. Uit een recent onderzoek door het Amerikaanse Towergate Insurance bleek dat vorig jaar maar liefst 97 procent van de ondervraagde kleinere ondernemingen in hun groeistrategie geen grote prioriteit geven aan de beveiliging van hun online activiteiten. Zij bleken de risico's ernstig te onderschatten: 82 procent van de mkb-eigenaars beweerden dat ze zich geen doelwit voelden voor een cyberaanval, omdat 'er toch niet veel de moeite van het stelen waard was'. Uit een ander onderzoek door een andere verzekeringsmaatschappij kwam naar voren dat slechts 23 procent van de mkb'ers zich 'ernstig zorgen maakt' over cyberrisico's en digitale inbraak.

MKB beveiliging

Een grotere organisatie met een ruimer budget kan snel en efficiënt handelen in geval van een digitale inbraak. Kleinere organisaties daarentegen hebben vaak het geld en de mankracht niet om zich adequaat voor te bereiden op een cyberaanval. Maar dat is geen excuus voor het negeren van die risico's: als je nu nog niet bent aangevallen, zal dat ooit wél gebeuren. Tegenwoordig is er veel meer data online, en ook veel meer hackers die proberen die data of systemen te kraken. Bovendien worden computers steeds sneller en hebben meer processcapaciteiten, dus kunnen hackers vergeleken met enkele jaren geleden exponentieel meer

hack-aanvallen uitvoeren. Het is daarom ook makkelijker om wachtwoorden te kraken.

Foutje

Enkele vergissingen die mkb'ers kunnen maken als het gaat om bescherming tegen een cyberaanval:

• Er geen rekening mee houden

Volgens het eerste hierboven genoemde onderzoek heeft 31 procent van de mkb-ondernemingen geen plan van actie om maatregelen te nemen tegen een cyberaanval, en zegt 22 procent dat ze niet weten hoe ze zich zouden kunnen wapenen tegen een aanval. De kans op een cyberaanval op elk formaat onderneming blijft groeien dankzij de ontwikkeling van de technologie en dus ook de hacking-technieken. Zonder een degelijk responsplan loop je dus een groot risico. Want de vraag is niet óf, maar wannéér zo'n aanval plaatsvindt.

• Er vanuit gaan dat je beschermd bent

Er bestaan bij mkb-ondernemingen twee grote misvattingen over fraude-bescherming. De ene is dat je bank je verlies wel zal dekken als de zakenrekening wordt geplunderd door een hacker. De andere is dat je verzekering die schade dekt. Beide zijn dus fout: banken dekken alleen privé-rekeningen, en verzekeringen dekken geen verliezen ontstaan door derdepartij service providers.

• De 'insiders' niet in de gaten houden

In een zakelijke omgeving verwacht je eigenlijk niet dat de medewerkers of zakenpartners je organisatie gaan benadelen. Maar de realiteit is anders: insider fraude gebeurt echt, en vaker dan je denkt. Volgens de Amerikaanse Association of Certified Fraud Examiners was insider fraude in 2014 verantwoordelijk voor een schadepost van in totaal $3,7 miljard wereldwijd.
Insider fraude is heel moeilijk te herkennen, maar het goed in de gaten houden van het gedrag van je medewerkers – en dan gaat het om ongewone dingen, afwijkend van het normale gedragspatroon van die persoon – kan een aanwijzing zijn.

• Niet investeren in beveiligingssoftware

De grootste fout die een organisatie kan maken met betrekking tot zijn cyberbescherming is: er geen hebben. Voor elke moderne onderneming is een robuuste beveiligingsoplossing een absolute must-have, met name bedrijven die veel of al hun transacties online uitvoeren. Dit geldt met name wanneer kleinere organisaties voor al hun zakelijke operaties hetzelfde device gebruiken.
Als je point-of-sale systeem draait op dezelfde computer als waarmee je de bedrijfs e-mail bijhoudt, en een medewerker klikt op een foute link, of opent een foute bijlage op die computer, dan geeft die persoon daarmee een hacker toegang tot alle klanteninformatie.

Wat je wel kunt doen

Er zijn verschillende types beveiligingssoftware op de markt, die verschillende mates van bescherming bieden. Antivirus software is de meest gebruikte, en die zal beschermen tegen de meeste soorten malware. Firewalls, die geïmplementeerd kunnen worden met hardware of software, bieden een extra beveiligingslaag doordat ze verhinderen dat een niet-geautoriseerde gebruiker toegang krijgt tot een computer of netwerk. Sommige computer operating systems, zoals Microsoft Windows, hebben ingebouwde firewalls, maar deze beschermingen kunnen ook apart worden toegevoegd aan routers en servers.
Ondernemingen zouden ook moeten investeren in een data backup oplossing, waarmee alle gecompromitteerde of verloren informatie kan worden teruggehaald vanuit een alternatieve locatie. Encryptie software beschermt gevoelige gegevens zoals medewerkersdossiers, klantengegevens en financiële bestanden.

Best practices

We geven enkele tips om je organisatie en je gegevens zo goed mogelijk te beschermen.

• Houd je software up-to-date

Wanneer je antivirus software of andere beveiligingsapplicatie meldt dat deze verloopt, of dat er een patch nodig is, laat die update dan niet wachten. Hackers scannen continu naar veiligheidslekken. Hoe langer je wacht met updaten, hoe groter de kans op inbraak.

• Instrueer je medewerkers

Als de medewerkers zich goed beseffen welke gevaren er op de digitale loer liggen, zijn ze daar ook op bedacht. Instrueer je mensen hoe ze een potentiële inbraak kunnen herkennen: laat ze zien hoe criminelen je systemen kunnen infiltreren.

• Implementeer een formeel beveiligingsbeleid

Als een organisatie in alle lagen een strak beleid heeft ingevoerd voor de beveiliging van de systemen, is de kans op een inbraak veel kleiner. Denk aan sterke wachtwoorden (combinaties van kleine en hoofdletters en cijfers en symbolen) die elke 60 of 90 dagen worden vervangen.

• Test je incident responsplan

Er van uitgaande dat je een responsplan hebt dat in werking treedt als zich een hack- of malware incident heeft voorgedaan, moet je dat ook uittesten met je medewerkers, zodat ze weten hoe te handelen.

Uiteindelijk het beste wat je kunt doen, is ervoor te zorgen dat iedereen zich bewust is van de mogelijke gevaren van een digitale inbraak. Een muisklik is snel gedaan, maar de gevolgen kunnen dramatisch zijn, voor grote, maar misschien nog wel meer voor kleinere ondernemingen. ■