BEVEILIG JE DATA

Zet het in de Cloud

ARTEQ

Het is tegenwoordig aan de orde van de dag dat deze of gene er niet in is geslaagd haar data afdoende te beschermen tegen ongenode gasten. Nog recent maakte Disney bekend dat hackers mogelijk toegang tot een van haar filmproducties hebben gekregen, waardoor het bedrijf grote financiële schade verwacht. Bovendien zijn we net bekomen van de Wannacry-schok waardoor minstens 200.000 systemen geïnfecteerd zijn geraakt. Wat is een goede strategie om uw data te beschermen?

IN CYBERCRIME GAAN MILJARDEN OM

In 2016 stond de teller wereldwijd op ruim 3000 veiligheidsincidenten[1]. Er kan rustig vanuit gegaan worden dat dit maar het topje van de ijsberg is. Bedrijven zijn voorzichtig om te rapporteren dat er mogelijk gegevens op straat liggen, of dat bedrijfsprocessen stoppen omdat applicaties niet bereikbaar zijn. Uiteraard bent u zeer zorgvuldig geweest en heeft u het nodige in veiligheid geïnvesteerd. U heeft firewalls en andere beschermingsmiddelen aangeschaft en specialisten geraadpleegd. Ondanks alle deze inspanningen is het toch niet gelukt om de hacker buiten de deur te houden.

Dat is ook niet zo vreemd; de markt is enorm en de belangen zijn bijzonder groot. De ransomware markt (waarbij data gegijzeld wordt door een derde middels b.v. een Wannacry-virus) wordt voor 2017 geschat op $400 miljoen. Phising mails om uw bankgegevens te krijgen zijn inmiddels niet meer van echt te onderscheiden. Daarnaast zijn er ook nog de cyber criminelen met andere doelstellingen zoals terrorisme of (economische) spionage, en hun methoden worden steeds verfijnder. De totale omvang van de cybercrime markt wordt geschat op $4.8 miljard.

WAPENWEDLOOP OP INTERNET

Helaas is er een grote groep criminelen die er belang bij heeft om bij uw systemen of data te komen, en daar ook hun vak van hebben gemaakt. Als u aangevallen wordt, moet u zich verdedigen. Helaas dient deze verdediging steeds geavanceerder te worden. Het lijkt op de wapenwedloop in het echte leven: steeds verdergaande en geavanceerdere aanvallen, iedere keer weer zwaardere verdedigingsmiddelen of antwoorden op deze aanvallen. De vraag om beveiligingsexperts explodeert.

[1] Zie http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2016/

Er zijn er maar weinig bedrijven in Nederland die zich de luxe kunnen veroorloven om hier afdoende antwoord op te geven want dit vereist gespecialiseerde personeel. Niet voor 5x8 maar 7x24, want de (cyber)attacks gaan dag en nacht door. [2]

ZET UW DATA IN DE CLOUD, DAAR IS HET VEILIGER

Het klinkt paradoxaal dat uw data in de cloud veiliger is. Als de data bij een cloud provider opgeslagen wordt, staat deze immers "midden op het Internet" en is dus een makkelijk doelwit voor cyber criminelen? Dat is maar gedeeltelijk waar.

Een (gerenommeerde) cloud provider heeft schaalgrootte en kan investeren in goede beveiligingsoplossingen en specialisten. Zo heeft het Europese ENISA een richtlijn voor Digital Service Providers opgezet om de veiligheid van de gegevens en diensten te waarborgen[3]. SIEM[4]- en DDoS[5]-analyses[6] zijn een aantal beveiligingsmethoden die effectief maar redelijk standaard zijn. Extra maatregelen zullen om voor de hand liggende redenen niet zo snel publiekelijk gemaakt worden: de hacker krijgt geen aanwijzing waar niet of juist wel een poging ondernomen kan worden om een gat in de verdediging te slaan.

"WEINIG BEDRIJVEN KUNNEN EEN AFDOENDE ANTWOORD TEGEN CYBERCRIME FORMULEREN"

De ENISA-richtlijnen gaan niet alleen over de technische beveiliging, maar ook organisatorisch. Hoe goed is de Digital Service Provider georganiseerd om een digitale aanval te weerstaan of ervan te herstellen. Zo voldoet de gemiddelde cloud provider aan een groot aantal beveiligings- en compliance standaarden, mogelijk zelfs beter dan waar de grootste bedrijven in Nederland (of buitenland: denk aan Sony of Disney) aan kunnen voldoen.

VERTROUW NIET OP DE VERDEDIGING; VERSLEUTEL UW DATA

Is de cloud provider immuun voor aanvallen? De toekomst zal het leren, maar feit is dat tot nog toe weinig verontrustende digitale inbraken bij DSP's zijn gerapporteerd. Hoewel ook hier aangenomen

---

[2] Daarnaast zijn ook fysieke beveiligingsuitdagingen, maar dit valt buiten de scope van dit artikel.
3 Zie www.enisa.europa.eu: Technical Guidelines for the implementation of minimum security measures for Digital Service Providers
4 Security Incident and Event Management Tools - correlaties en patronen in het in/uitgaande verkeer aanbrengen waardoor mogelijk schadelijk gedrag vroegtijdig ontdekt en onschadelijk gemaakt kan worden
5 DDOS – Distributed Denial of Service, een massale aanval op uw Website waardoor deze niet meer bereikbaar is voor uw klanten

mag worden dat een cyberattack niet van de daken geschreeuwd zal worden, zal een cloud provider zijn reputatie niet op het spel willen zetten en sneller openkaart spelen.

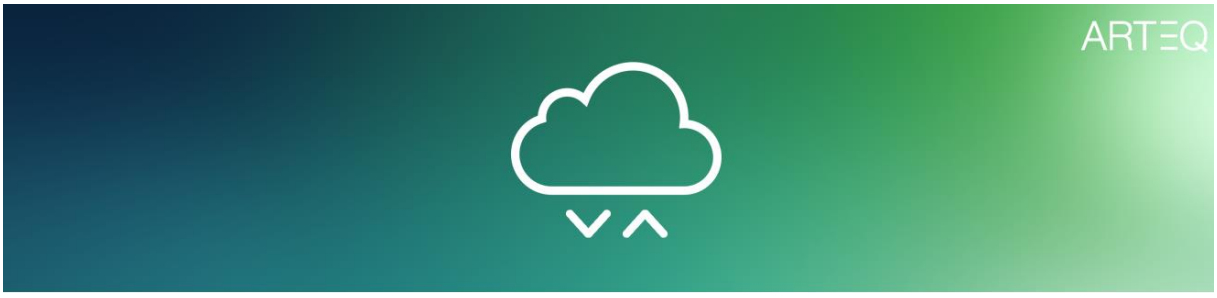
Daarnaast bieden de betere cloud providers standaard aan om de data zowel tijdens transport (al dan niet over publiek internet) als in rust (opgeslagen op disk) te versleutelen waarbij de sleutel in handen is van de klant. Hoewel veel door bedrijven aangeschafte opslagsystemen standaard deze encryptie-mogelijkheden bieden wordt het in de praktijk zelden noodzakelijk gevonden dit ook daadwerkelijk toe te passen. In de cloud of niet, maak gebruik van deze mogelijkheid waardoor de succesvolle cyberattacker in ieder geval de data nog dient te ontcijferen.

HOE STAAT HET MET UW INTERNE BEVEILIGING?

Wat niet veranderd is het beveiligingsvraagstuk van binnenuit. Geschat wordt dat 75% van de veiligheidsincidenten door de gebruikers veroorzaakt worden, en dat is in de cloud niet anders. Veiligheid is immers een aaneenschakeling van processen en middelen, waarbij de zwakste schakel bepaald hoe goed de totale beveiliging geregeld is.

Vaak zijn eindgebruikers onachtzaam, programma's of werkplekken onvoldoende beveiligd, of probeert een eindgebruiker bewust ongeautoriseerde toegang tot gegevens te krijgen. Als niet de juiste interne maatregelen genomen zijn kan het Wannacry-virus alsnog uw gegevens in de cloud gijzelen.

Door de zorg voor het afslaan van externe aanvallen aan de cloud provider over te laten, krijgt uw organisatie ruimte om meer aandacht aan de interne veiligheid te besteden.Ondertussen kunt u een volgende stap zetten in de afbouw van het peperdure datacenter, waardoor er meer budget vrijkomt om aan de échte IT-vraagstukken te wijden.



Meer weten over Cloud? U kunt vrijblijvend contact opnemen met Wim Huijbers: wim.huijbers@arteq.nl of 06-54966728.