DDoS-Aanvallen en rol van Interne Audit Functie

8 december 2020

Gülnur Orpak, Kunter Orpak

***Distributed denial of service* (DDoS) is een vorm van *DoS* waarbij een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal verschillende bronnen ('distributed'). [NCTV20] Het resultaat is dat deze diensten slecht of helemaal niet meer bereikbaar zijn voor medewerkers of klanten van een organisatie. Een DDoS-aanval kan daarmee de ICT en de daarvan afhankelijke processen van een organisatie verstoren. Criminelen zetten dit soort aanvallen meestal in om via afpersing geld te verdienen door organisaties te dreigen met een aanval.**

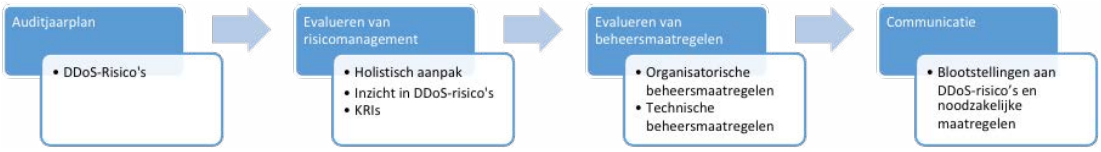
Incidenten bij financiële instellingen

Omdat de slagingskans en schade van een DDoS-aanval in het algemeen vrij groot is [NCSC16a], zijn financiële markten interessante targets voor criminelen. Volgens een onderzoeksrapport van Akamai was meer dan 40 procent van de DDoS-aanvallen in 2018 en 2019 gericht op financiële instellingen. [AKAM20] Bovendien steeg de afgelopen drie jaar het percentage van de DDoS-incidenten bij financiële instellingen wereldwijd met 32 procent. [ZDNE20] Het opvallendste incident in 2020 was dat bij de Nieuw-Zeelandse aandelenbeurs (NZX). De NZX werd in augustus 2020 twee dagen achter elkaar platgelegd door een DDoS-aanval, waardoor het niet meer mogelijk was om te handelen. [SECU20]

Deze incidenten leiden onontkoombaar tot een pijnlijke vraag: lopen financiële instellingen in Nederland steeds meer het risico te worden getroffen door DDoS-aanvallen?
Volgens een publicatie van het Nationaal Cyber Security Centrum (NCSC) ontvingen verschillende organisaties afpersingmails waarin wordt gedreigd met een DDoS-aanval [NCSC20] Uit deze publicatie blijkt dat het volume van de DDoS-aanvallen voor Nederlandse maatstaven uitzonderlijk groot is en de aanvallen tot 250 Gbps (Gigabit per seconde) kunnen oplopen. Ter indicatie: in 2019 was de grootste aanval in Nederland 124 Gbps. Het volume per aanval neemt dus flink toe.

Rol van de Interne Audit Functie

Interne audit functies (IAF) dragen bij aan de realisatie van de organisatiedoelstellingen. Als objectieve waarnemer verschaffen ze aanvullende zekerheid over de effectiviteit en de beheersing van de bedrijfsvoering. Hun taak omvat uitvoeren van audits en het senior management, het bestuur en de auditcommissie hierover rapporteren en adviseren. Daarom kunnen de IAF's toegevoegde waarde leveren door de toetsing van de DDoS-beheersmaatregelen die zijn getroffen om de continuïteits- en beschikbaarheidsdoelstellingen in de financiële instellingen te realiseren.
Zie figuur 1.



Figuur 1: Rol interne auditfunctie

Auditjaarplan

IAF's moeten een op risicoanalyse gebaseerd auditjaarplan opstellen om de prioriteiten van de IAF te bepalen (IIA Standaarden 2010 – Planning). [IIA07] Deze risico's worden gewogen in het licht van de doelstellingen van de organisatie. Gezien de omvang van de dreiging kunnen IAF's in hun risicoanalyse voor het jaar 2021 toenemende DDoS-risico's bij de financiële instellingen in overweging nemen.

Evalueren risicomanagement

IAF's zijn verantwoordelijk voor de beoordeling van de effectiviteit van de processen (risicomanagement- en -beheersmaatregelen) in organisaties. Interne auditors bij financiële instellingen kunnen het management een holistische aanpak bieden door de kwetsbaarheden voor DDoS-aanvallen te identificeren en de toereikendheid van detecterende maatregelen en herstelwerkzaamheden te toetsen. Zo kunnen Interne auditors het management inzicht verschaffen in de DDoS-risico's op de bedrijfsprocessen, systemen, assets en data.

In het kader van de consulting-rol van interne audit kunnen IAF's samenwerken met de ICT-afdeling en de informatiebeveiligingsafdeling om de *key risk indicators* (KRIs) rondom het DDoS-domein te ontwikkelen en monitoren. [IIA15]

Evalueren beheersmaatregelen

Het NCSC adviseert om zowel technische als organisatorische maatregelen te treffen als bescherming tegen DDoS-aanvallen. [NCSC16a] Een DDoS-aanval is niet helemaal te voorkomen. Het werk van de interne auditor richt zich dan ook niet zozeer op de maatregelen die zijn getroffen om DDoS aanvallen te voorkomen, maar vooral op de doeltreffendheid en doelmatigheid van de technische en organisatorische beheersmaatregelen die getroffen zijn om de impact van DDoS-aanvallen te beperken en om de processen en systemen te herstellen na een DDoS-aanval.

Organisatorische beheersmaatregelen

Preventief moeten organisaties processen implementeren in lijn met hun informatiebeveiligingsbeleid, om DDOS-risico's te identificeren en te beheersen. Voor de inrichting van processen die DDOS-bedreigingen detecteren, kunnen financiële instellingen gebruikmaken van internationaal geaccepteerde raamwerken zoals MITRE ATT&CK [MITR20]. Financiële instellingen moeten ook processen inrichten en plannen vaststellen die worden geactiveerd bij detectie van een DDoS-incident. Deze processen en plannen bevatten in elk geval maatregelen om het incident te stoppen, de negatieve impact te beperken, de schade te herstellen en hier goed over te communiceren met stakeholders. [AFM19] In het kader van de organisatorische maatregelen kunnen de IAF's bij financiële instellingen het bestuur redelijke zekerheid bieden over de doeltreffendheid van de processen voor *threat intelligence*, logging en monitoring, capaciteitsmanagement, incidentmanagement en businesscontinuïteit. Maar alleen de organisatorische maatregelen zijn niet toereikend om de DDoS-risico's te mitigeren, er zijn ook technische maatregelen nodig.

Technische beheersmaatregelen

Interne auditors moeten voldoende kennis bezitten van de belangrijkste informatietechnologische risico's en beheersmaatregelen om de hen toegewezen werkzaamheden te kunnen uitvoeren (IIA Standaarden 1210.A3). [IIA07] Financiële instellingen moeten meerdere technische maatregelen treffen om de ICT-infrastructuur te beschermen tegen DDoS-aanvallen. [NCSC16b] Enkele voorbeelden zijn *system hardening*, het doorvoeren van de meest recente updates en het gebruik van *web application firewalls, dedicated network firewalls* en *loadbalancers*. IAF's kunnen het bestuur redelijke zekerheid bieden dat de benodigde technische maatregelen zijn opgenomen in verschillende lagen van de infrastructuur, zoals applicaties, diensten, servers en netwerk en dat deze maatregelen doeltreffend zijn. Startpunt hiervoor is de risicoanalyse van DDoS-dreigingen en technische analyses door de ICT-afdeling en de informatiebeveiligingsafdeling. Het toetsen of de beveiligingsconfiguraties in het netwerk overeenstemmen met best practices en interne baselines kan een goed begin zijn om het beveiligingsniveau van de internet-verbonden componenten indirect omhoog te brengen.

Communicatie met bestuur

Het hoofd van de IAF moet in de periodieke en ad-hocrapportages aan directie en rvc de belangrijkste DDoS-risico's en ontbrekende maatregelen onder de aandacht brengen. De inhoud van de rapportages hangt af van de potentiele impact van DDoS-aanvallen en daarmee de hoogte van het risico en de mate van urgentie voor het nemen van maatregelen door het senior management en het bestuur (IIA Standaard 2060) [IIA07].

Samenvatting aanbevelingen

Interne auditors bij financiële instellingen kunnen veel betekenen om DDoS-risico's te mitigeren. Hieronder zijn de aanbevelingen voor de IAF's uit dit artikel samengevat:

- Neem de toenemende DDoS-risico's op in het audit universe.
- Help het management om de DDoS-kwetsbaarheden te identificeren door audit- en consulting-opdrachten.
- Toets de doeltreffendheid van de organisatorische maatregelen in processen zoals *threat intelligence*, logging en monitoring, capaciteitsmanagement, incidentmanagement en businesscontinuïteitsmanagement en rapporteer hierover aan het bestuur.
- Evalueer de genomen technische maatregelen in verschillende lagen van de infrastructuur in overeenstemming met het advies van het NCSC.
- Breng de belangrijkste blootstellingen aan DDoS-risico's en noodzakelijke maatregelen onder de aandacht van het bestuur.

Literatuur

[AFM19], '*AFM publiceert Principes voor Informatiebeveiliging*', 2019, https://www.afm.nl/nl-nl/nieuws/2019/dec/principes-informatiebeveiliging, geraadpleegd op 12 november 2020.

[AKAM20] Akamai, '*State of the Internet/Security: Financial Services – Hostile Takeover Attempts*', 2020, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf, geraadpleegd op 12 november 2020

[IIA07] IIA – Instituut van Internal Auditors, '*De internationale standaarden voor de beroepsuitoefening van internal auditing*', 2007, https://www.iia.nl/SiteFiles/Standaarden%20NL.pdf, geraadpleegd op 12 november 2020.

[IIA15] IIA – The Institute of Internal Auditors, '*Internal Audit's Role in Cyber Preparedness*', 2015, http://theiia.mkt5790.com/Cyber_Preparedness/?sessionGUID=4725dd08-ac9b-d126-7375-cbe7a31ac0d1&webSyncID=9ba3b403-55c6-70e8-0848-2658caeec3c0&sessionGUID=97c9ce4b-e751-e1a3-2894-d679a004cac3, geraadpleegd op 12 november 2020.

[MITR20] MITRE– MITRE ATT&CK® Matrix for Enterprise, '*Enterprise Matrix*', 2020, https://attack.mitre.org/matrices/enterprise/, geraadpleegd op 27 oktober 2020.

[NCSC16a] NCSC – Nationaal Cyber Security Centrum, '*Continuïteit van onlinediensten*', 2016, https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten, geraadpleegd op 12 november 2020.

[NCSC16b] NCSC – Nationaal Cyber Security Centrum, '*Factsheet Technische maatregelen voor de continuïteit van onlinediensten*', 14 maart 2016, https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-technische-maatregelen-voor-continuiteit-van-online-diensten, geraadpleegd op 12 november 2020.

[NCSC20] NCSC – Nationaal Cyber Security Centrum, '*Toename aan intensiteit en aantal DDoS-aanvallen*', 2020, https://www.ncsc.nl/actueel/nieuws/2020/september/4/toename-aan-intensiviteit-en-aantal-ddos-aanvallen, geraadpleegd op 12 november 2020.

[NCTV20] NCTV – Nationaal Coördinator Terrorismebestrijding en Veiligheid, '*Cybersecuritybeeld Nederland (CSBN) 2020*', https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020, geraadpleegd op 12 november 2020.

[SECU20] Security.nl, '*Nieuw-Zeelandse aandelenbeurs NZX platgelegd door ddos-aanval*', 2020, https://www.security.nl/posting/669067/Nieuw-Zeelandse+aandelenbeurs+NZX+platgelegd+door+ddos-aanval, geraadpleegd op 12 november 2020.

[ZDNE20] ZDNet, '*Financial sector is seeing more credential stuffing than DDoS attacks*', 2020, https://www.zdnet.com/article/financial-sector-has-been-seeing-more-credential-stuffing-than-ddos-attacks-in-recent-years/, geraadpleegd op 12 november 2020.

Gülnur Orpak CISA, CIA, ISO27001LA | Senior interne auditor bij *ABN Amro*

Gülnur Orpak is werkzaam als senior IT-auditor bij ABN Amro en heeft tien jaar ervaring in de financiële markten. Ze heeft diverse auditwerkzaamheden uitgevoerd bij verschillende financiële instellingen, onder andere op het gebied van informatiebeveiliging, uitbesteding en PSD2. Gülnur is lid van de IIA Nederland en de ISACA NL Chapter.

Kunter Orpak CISA, CIA, ISO27001LA, CSX-F, CFSA, CCSA | Toezichthouder bij de *Autoriteit Financiële Markten*

Kunter Orpak werkt bij de Autoriteit Financiële Markten als toezichthouder op het gebied van operationele en ICT-risico's, waaronder informatiebeveiligingsrisico's. Hij is voornamelijk actief in het toezicht op de kapitaalmarkten. Kunter heeft meerdere jaren ervaring als interne auditor bij verschillende financiële instellingen. Kunter is lid van de IIA Nederland en de ISACA NL Chapter.