Samenvatting

Cisco-beveiligingsrapport 2015

Het moderne bedreigingslandschap is dynamisch, maar toch zijn er enkele constanten:

Kwaadwillenden verfijnen continu technieken of ontwikkelen nieuwe technieken die detectie kunnen vermijden en kwaadaardige activiteiten kunnen verbergen. De verdedigers – beveiligingsteams – moeten continu hun aanpak verbeteren om de organisatie en gebruikers tegen deze steeds geraffineerdere campagnes te beschermen.

De gebruikers zitten tussen twee vuren. Maar nu blijkt dat ze niet alleen doelwit zijn, maar ook medeplichtig zijn aan de uitvoering van aanvallen.

In het *Cisco-beveiligingsrapport 2015*, met de onderzoeksresultaten, inzichten en perspectieven van Cisco® Security Research en andere beveiligingsexperts binnen Cisco, wordt de voortgaande strijd tussen aanvallers en verdedigers beschreven en wordt aangegeven hoe gebruikers een steeds zwakkere schakel in de beveiligingsketen vormen.

Cyberbeveiliging is een brede, complexe zaak en kan verstrekkende gevolgen hebben voor gebruikers, bedrijven, overheden en andere groepen wereldwijd. Het *Cisco-beveiligingsrapport 2015* is opgedeeld in vier discussiegebieden. Deze secties en de problemen die daarin worden verkend, lijken in eerste instantie op zichzelf staand, maar bij nader onderzoek blijkt dat ze wel degelijk zijn verbonden:

Vier discussiegebieden van het *Cisco-beveiligingsrapport 2015:*

1. Informatie over bedreigingen
2. Security Capabilities Benchmark Study
3. Geopolitieke trends en branchetrends
4. Het beeld van cyberbeveiliging veranderen – van gebruikers tot de directiekamer

Download het Cisco-beveiligingsrapport 2015 op www.cisco.com/go/asr2015

1. Informatie over bedreigingen

Deze sectie biedt een overzicht van het meeste recente bedreigingsonderzoek van Cisco, waaronder updates over exploitkits, spam, bedreigingen en kwetsbaarheden, en trends op het gebied van malvertising (kwaadaardige advertenties). De trend dat online criminelen steeds vaker misbruik maken van gebruikers om hun aanvallen uit te voeren, is ook onderzocht. Cisco Security Research heeft een wereldwijde set telemetriegegevens gebruikt om de analyse van waargenomen trends in 2014 te produceren. De informatie over bedreigingen die in het rapport is opgenomen, omvat bijdragen van topbeveiligingsexperts bij diverse afdelingen van Cisco.

2. Security Capabilities Benchmark Study

Cisco heeft de perceptie van beveiligingsprofessionals van de beveiligingstoestand binnen hun organisaties gepeild door CISO's (Chief Information Security Officers) en SecOps-managers (Security Operations) in negen landen en bij zowel grote als kleine bedrijven te vragen naar hun beveiligingsresources en -procedures. De bevindingen van dit onderzoek worden exclusief gepresenteerd in het *Cisco-beveiligingsrapport 2015*.

3. Geopolitieke trends en branchetrends

In deze sectie worden door Cisco-experts op het gebied van beveiliging, geopolitiek en beleid huidige en opkomende geopolitieke trends geïdentificeerd die organisaties – met name multinationals – zouden moeten monitoren. Er wordt ingegaan op de groei van cybercriminaliteit in gebieden met zwakke governance. Tevens worden recente wereldwijde ontwikkelingen ten aanzien van de soevereiniteit, lokalisatie, encryptie en compatibiliteit van gegevens beschreven.

4. Het beeld van Cyberbeveiliging veranderen – van gebruikers tot de directiekamer

Beveiligingsexperts van Cisco voeren aan dat het tijd is voor organisaties om hun aanpak van cyberbeveiliging te veranderen als zij beveiliging in de echte wereld willen bewerkstelligen. Strategieën omvatten het adopteren van geavanceerdere beveiligingsmechanismen om zich te verdedigen tegen bedreigingen voor, tijdens en na een aanval, beveiliging tot onderwerp maken op de agenda in de directiekamer en het implementeren van het Cisco-beveiligingsmanifest: een set beveiligingsprincipes waarmee organisaties hun aanpak van beveiliging dynamischer kunnen maken – en zich beter kunnen aanpassen en sneller kunnen innoveren dan kwaadwillenden.

Het onderlinge verband van de beveiligingsonderwerpen die in het *Cisco-beveiligingsrapport 2015* aan bod komen is als volgt: aanvallers worden steeds beter in het misbruik maken van tekortkomingen in de beveiliging om hun kwaadaardige activiteiten te verbergen en verhullen. Gebruikers – en beveiligingsteams – vormen deel van het beveiligingsprobleem. Hoewel vele verdedigers van mening zijn dat hun beveiligingsprocessen geoptimaliseerd zijn – en de beveiligingstools effectief – behoeft hun beveiligingsgereedheid naar alle waarschijnlijkheid verbetering. Wat plaatsvindt binnen het geopolitieke landschap, van wetgeving tot beveiligingsbedreigingen, kan een rechtstreekse impact hebben op bedrijfsactiviteiten en op de manier waarop organisaties beveiliging aanpakken. Wanneer al deze factoren in overweging worden genomen, blijkt dat het voor organisaties essentiëler is dan ooit om te beseffen dat beveiliging een 'mensenprobleem' is, dat er altijd sprake is van risico's en dat het nu tijd is voor een nieuwe aanpak van beveiliging.

Hoofdkantoor Amerika
Cisco Systems Inc.
San Jose, CA

Hoofdkantoor Zuidoost-Azië
Cisco Systems (USA) Pte. Ltd.
Singapore

Hoofdkantoor Europa
Cisco Systems International BV
Amsterdam, Nederland

Cisco beschikt wereldwijd over meer dan 200 kantoren. Adressen, telefoonnummers en faxnummers vindt u op de Cisco-website op www.cisco.com/go/offices.