Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

01-12-2025:

Europese landen bespreken gezamenlijke cyberaanvallen als reactie op Russische hybride dreiging

Europese landen onderzoeken nieuwe manieren om gezamenlijk op te treden tegen hybride aanvallen die aan Rusland worden toegeschreven. Volgens berichten overwegen meerdere lidstaten offensieve cyberoperaties uit te voeren, gecoördineerd via Europese of NAVO kanalen. Deze mogelijke aanpak richt zich op digitale systemen die van strategisch belang zijn voor de Russische oorlogsvoering. De plannen maken deel uit van een bredere discussie over het versterken van het collectieve antwoord op digitale sabotage, desinformatie, GPS verstoringen en fysieke aanvallen op kritieke infrastructuur in Europa.

Sinds het uitbreken van de oorlog in Oekraïne is het Europese dreigingsbeeld aanzienlijk veranderd. Hoewel het militaire conflict zich vooral afspeelt op Oekraïens grondgebied, ervaren verschillende Europese landen een toename van digitale en hybride activiteiten die worden gezien als pogingen om democratische instellingen te ondermijnen. Daarbij worden onder meer sabotage, grensprovocaties en digitale spionage genoemd. De grens tussen digitale oorlogsvoering en fysieke risico’s wordt volgens Europese diplomatieke bronnen steeds dunner.

Binnen de NAVO groeit de aandacht voor asymmetrische maatregelen als onderdeel van de strategische communicatie en afschrikking. Europese regeringen verkennen de mogelijkheid van snelle, gezamenlijke reactieprocedures, waaronder het direct publiek toeschrijven van digitale aanvallen aan een tegenstander. Daarbij wordt gesproken over het versnellen van de besluitvorming en het verbeteren van de informatie-uitwisseling tussen lidstaten om nauwkeuriger te kunnen reageren op cyberaanvallen en hybride acties.

Latvia en Italië hebben voorstellen ingediend voor verdergaande militaire en digitale coördinatie, waaronder een permanent Europees centrum voor hybride dreigingen en een gezamenlijke cybermacht gericht op offensieve capaciteiten. Daarnaast wordt gesproken over de inzet van specialisten op het gebied van kunstmatige intelligentie en geavanceerde data-analyse, waarmee de detectie en attributie van aanvallen sneller moet verlopen.

De discussie laat zien dat digitale oorlogsvoering een structureel onderdeel is geworden van de veiligheidsstrategie van Europa. Het versterken van digitale

weerbaarheid en de mogelijkheid tot gezamenlijke offensieve respons vormen toekomstige kernpunten van Europees veiligheidsbeleid.

Rusland dreigt met blokkade van WhatsApp

De Russische telecomwaakhond Roskomnadzor heeft opnieuw gedreigd met een volledige blokkade van WhatsApp, tenzij het platform voldoet aan de eisen van de Russische wetgeving. Deze dreiging volgt op eerdere beperkingen die werden opgelegd aan WhatsApp en Telegram, waarbij Rusland beschuldigt dat deze platforms niet genoeg meewerken met de wetshandhaving, vooral bij zaken van fraude en terrorisme.

Deze situatie benadrukt de groeiende controle van Rusland over digitale communicatiekanalen, waarbij apps zoals WhatsApp steeds vaker het doelwit zijn van overheidsmaatregelen. WhatsApp zelf heeft verklaard dat dit beleid de toegang tot veilige communicatie voor miljoenen Russen kan ondermijnen. Het conflict heeft al geleid tot de volledige blokkade van andere berichtenplatformen zoals Signal en Viber in 2024. De Russische autoriteiten steunen ook hun eigen berichtenapp MAX, waarvan wordt gevreesd dat deze wordt gebruikt om gebruikersgedrag te monitoren, hoewel deze beschuldigingen door staatsmedia worden ontkend.

De ontwikkelingen in Rusland hebben een bredere implicatie voor digitale communicatie wereldwijd, omdat ze een trend weerspiegelen waarbij overheden meer controle willen uitoefenen over de platforms die de digitale interactie van hun burgers vormen. Dit is een ontwikkeling waar zowel Europese landen, waaronder Nederland en België, mogelijk mee te maken krijgen, vooral in het licht van de groeiende bezorgdheid over privacy en digitale rechten in een steeds meer gecentraliseerde online omgeving.

Onderzoek toont aan dat X-algoritme polarisatie vergroot: impact op digitale veiligheid

Een recent wetenschappelijk onderzoek gepubliceerd in Science heeft aangetoond hoe het algoritme van het sociale-mediaplatform X (voorheen Twitter) bijdraagt aan de vergroting van polarisatie onder gebruikers. Het onderzoek, uitgevoerd onder 1000 gebruikers, toont aan dat de gepersonaliseerde 'For You'-feed van het platform de blootstelling aan polariserende en antidemocratische standpunten vergroot, wat

leidt tot een versnelde polarisatie van opvattingen binnen slechts een week. Dit proces is bijzonder relevant voor digitale veiligheid, omdat het de dynamiek van desinformatie en de versterking van extremistische opvattingen kan beïnvloeden, wat ook gevolgen heeft voor cyberdreigingen en de online weerbaarheid van gebruikers.

In Nederland en België, waar sociale-mediaplatforms een belangrijke rol spelen in de verspreiding van informatie, zou het manipuleren van de gebruikerservaring via algoritmes kunnen bijdragen aan een verstoorde informatie-omgeving. Het onderzoek wijst op de kracht van algoritmes om niet alleen de publieke opinie te beïnvloeden, maar ook de risico's van manipulatie door kwaadwillende actoren te vergroten. Dergelijke technologieën kunnen dienen als platformen voor desinformatiecampagnes, wat in de context van cyberdreigingen en hybride oorlogvoering een ernstig risico vormt.

Hoewel de resultaten van het onderzoek suggereren dat platforms de polarisatie kunnen verminderen door hun algoritmes aan te passen, benadrukt het ook de verantwoordelijkheid van platformen zoals X om hun algoritmes transparanter te maken en misbruik van dergelijke technologieën te voorkomen. Dit is essentieel voor het beschermen van de digitale soevereiniteit en de veiligheid van gebruikers in een tijd van toenemende digitale dreigingen.

Actief misbruik van kwetsbaarheid in OpenPLC ScadaBR ontdekt

De Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) heeft een kwetsbaarheid in de OpenPLC ScadaBR-software toegevoegd aan het 'Known Exploited Vulnerabilities' (KEV)-catalogus. Deze kwetsbaarheid betreft een cross-site scripting (XSS) probleem, aangeduid als CVE-2021-26829, die zowel de Windows- als Linux-versies van de software treft. De kwetsbaarheid, met een CVSS-score van 5.4, bevindt zich in het systeeminstellingenbestand en beïnvloedt OpenPLC ScadaBR-versies tot 1.12.4 voor Windows en 0.9.1 voor Linux.

CISA heeft deze kwetsbaarheid opgenomen in het KEV-lijst omdat er actief misbruik van wordt gemaakt. Dit werd eerder dit jaar opgemerkt toen een pro-Russische hacktivistengroep, TwoNet, het doelwit was van een honeypot simulatie, waarbij de aanvallers de XSS-kwetsbaarheid gebruikten om een pop-upmelding te plaatsen en systeeminstellingen te wijzigen. De aanval resulteerde in het aanpassen van de loginpagina en het uitschakelen van logs en alarmen. Deze aanvallers gaven aan

toegang te verkrijgen via standaardreferenties en voerden later verkenning en persistentieactiviteiten uit.

Als gevolg van dit misbruik is het voor federale civiele uitvoeringsorganen verplicht om voor 19 december 2025 de benodigde patches toe te passen voor een adequate bescherming. De aanvallen wijzen op een bredere inzet van industriële systemen door hacktivisten en andere cybercriminelen, met de inzet van hulpmiddelen zoals OAST (Out-of-Band Application Security Testing) voor exploitatie van kwetsbaarheden. De aanvalsgroep TwoNet heeft zich in januari 2025 gepositioneerd om industriële systemen aan te vallen, aanvankelijk gericht op DDoS-aanvallen en later uitgebreid naar ransomware-as-a-service en andere commerciële cyberactiviteiten. Dit benadrukt de noodzaak van extra waakzaamheid en het bijwerken van kwetsbare systemen om verdere aanvallen te voorkomen.

Overzicht van misbruikte kwetsbaarheden door hackers in Nederland, België en wereldwijd

Het afgelopen kwartaal heeft een aantal ernstige kwetsbaarheden blootgelegd die door hackers wereldwijd worden misbruikt, zowel in Nederland als België. Deze kwetsbaarheden zijn vooral gerelateerd aan veelgebruikte software en netwerkapparaten, waaronder routers, servers en verschillende populaire applicaties. De lijst van misbruikte kwetsbaarheden bevat een aantal die specifiek gericht zijn op IoT-apparaten, maar ook op belangrijke softwarecomponenten die in verschillende sectoren worden ingezet, van overheidsinstellingen tot grote bedrijven en consumenten.

Een van de meest voorkomende kwetsbaarheden betreft Metabase (CVE-2023-38646), een open-source business intelligence tool die wordt gebruikt door organisaties van verschillende groottes, van startups tot universiteiten. Deze kwetsbaarheid is in de afgelopen 30 dagen wereldwijd gezien bij 52 unieke IP-adressen in Nederland, wat aangeeft dat deze kwetsbaarheid vaak wordt aangewend door aanvallers. Daarnaast wordt de Cisco RV320/RV325 router (CVE-2019-1653), veelgebruikt door KMO's en thuisgebruikers, vaak aangevallen, ondanks het feit dat er sinds de ontdekking al een patch beschikbaar is. Ook Huawei's Home Gateway (CVE-2017-17215), een veelgebruikte router voor internetverbindingen in huishoudens en kleine bedrijven, wordt nog steeds actief aangevallen.

De lijst bevat ook kwetsbaarheden in applicaties zoals Apache HTTP Server (CVE-2021-42013), die wordt gebruikt door zowel grote ondernemingen als kleinere bedrijven om websites en webapplicaties te hosten. De voortdurende exploitatie van deze kwetsbaarheden benadrukt de noodzaak voor regelmatige updates en patches, aangezien aanvallers actief misbruik maken van bekende zwakke plekken om ongeautoriseerde toegang te verkrijgen en gegevens te stelen.

De kwetsbaarheid in SolarWinds Serv-U (CVE-2024-28995), een bestandsoverdrachtsoplossing die door veel organisaties wordt gebruikt voor veilige bestandoverdracht, is ook een belangrijke zorg. Na de bekende supply chain-aanval op SolarWinds in 2020, blijft deze software een aantrekkelijk doelwit voor cybercriminelen, vooral gezien het potentiële risico van datalekken. In de recente meldingen is de exploitatie van deze kwetsbaarheid gesignaleerd, vooral in België, met aanzienlijke dreigingen voor zowel overheidsinstellingen als private organisaties.

Deze kwetsbaarheden illustreren de voortdurende dreiging die gepaard gaat met het niet up-to-date houden van systeemsoftware en apparaten. Het is essentieel voor organisaties in zowel de publieke als de private sector om beveiligingspatches tijdig toe te passen en kwetsbare systemen regelmatig te controleren op tekenen van misbruik.

Top 10 trending CVE's: Kritieke kwetsbaarheden in populaire software en hardware

In de afgelopen 24 uur zijn verschillende kwetsbaarheden in software en hardware trending geworden op sociale media, die aanzienlijke aandacht krijgen van beveiligingsexperts. Deze kwetsbaarheden, die variëren van geheugenbeveiliging tot SQL-injecties, brengen grote risico’s met zich mee voor gebruikers wereldwijd, inclusief bedrijven en overheden. De hoogste prioriteit ligt bij de CVE's die betrekking hebben op kritieke toegangscodezwaktes en mogelijke externe code-executie.

Een van de opvallendste kwetsbaarheden is CVE-2025-21479, die betrekking heeft op de Graphics component van Qualcomm’s Adreno GPU-driver. Deze kwetsbaarheid kan leiden tot geheugencorruptie door ongeautoriseerde uitvoering van commando's in de GPU-microcode, wat aanzienlijke gevolgen kan hebben voor systemen die deze component gebruiken. De 'hype score' van deze CVE is 8.6, wat wijst op een grote bezorgdheid in de beveiligingsgemeenschap.

Andere belangrijke kwetsbaarheden die veel aandacht trekken zijn CVE-2025-13315 en CVE-2025-12421, die respectievelijk toegangscode-inbreuken in Twonky Server en Mattermost vertegenwoordigen. Beide kwetsbaarheden kunnen leiden tot het uitlekken van gevoelige gegevens of zelfs volledige accountovername. De hoge scores van deze CVE's geven aan dat ze als bijzonder gevaarlijk worden beschouwd.

Verder is er de SQL-injectiekwetsbaarheid in de Slider & Popup Builder plugin voor WordPress, die wordt aangeduid als CVE-2025-2011, welke aanvallers in staat stelt om gevoelige informatie uit databases te extraheren. Dit type kwetsbaarheid komt vaak voor in populaire plugins, wat het risico voor gebruikers verhoogt.

De lijst wordt verder aangevuld met een aantal andere kwetsbaarheden, waaronder een XXE-kwetsbaarheid in GeoServer (CVE-2025-58360) en een ernstige kwetsbaarheid in FreePBX (CVE-2025-57819), die aanvallers in staat stelt om op afstand willekeurige databasebewerkingen uit te voeren.

Gezien de variëteit aan software en systemen die getroffen kunnen worden door deze kwetsbaarheden, wordt het dringend aanbevolen voor organisaties en gebruikers om de laatste patches en updates van de betrokken softwareleveranciers te implementeren om risico’s te minimaliseren.

Man krijgt 7 jaar gevangenisstraf voor WiFi-aanvallen tijdens vluchten in Australië

Een 44-jarige man uit Australië is veroordeeld tot zeven jaar en vier maanden gevangenisstraf voor het uitvoeren van een "evil twin" WiFi-aanval. De man richtte zich op nietsvermoedende reizigers tijdens binnenlandse vluchten en op luchthavens in Australië, waar hij een nep-WiFi-netwerk opzet om persoonlijke gegevens te stelen. Deze aanvallen, die wereldwijd mogelijk zijn, benadrukken de risico's die verbonden zijn aan het gebruik van openbare WiFi-netwerken, iets waar ook reizigers in Nederland en België mee te maken kunnen krijgen.

Door het opzetten van een valse toegangspoort met dezelfde naam als de legitieme netwerken op luchthavens in steden zoals Perth, Melbourne en Adelaide, wist de man gebruikers naar een phishingpagina te leiden. De gestolen gegevens werden gebruikt om toegang te krijgen tot de social media-accounts van vrouwen, waaruit privé-informatie en beelden werden gestolen. Het onderzoek van de Australische autoriteiten leidde tot de ontdekking van duizenden gestolen gegevens.

Hoewel dergelijke "evil twin"-aanvallen relatief zeldzaam zijn, kunnen ze gevaarlijk zijn voor reizigers die onzorgvuldig omgaan met openbare netwerken. Experts waarschuwen voor het gebruik van VPN's en het vermijden van verdachte netwerken, vooral in luchthavens, hotels en andere openbare plaatsen. Deze zaak onderstreept het belang van bewustzijn en voorzorgsmaatregelen om je persoonlijke gegevens te beschermen tegen cybercriminelen.

Man aangehouden voor grootschalige uitgifte van vervalsingen via Darkweb

In Duitsland is een 36-jarige man aangehouden wegens de vervalsing van identiteitsbewijzen. De verdachte zou verantwoordelijk zijn voor het vervaardigen van valse documenten, die hij via het Darkweb aan klanten verkocht. De man werd in het district Jerichower Land in Sachsen-Anhalt gearresteerd en wordt beschuldigd van grootschalige vervalsingen, met minimaal 50 gevallen op zijn naam. De documenten werden verkocht voor prijzen tot 550 euro per stuk, waarbij klanten konden betalen met cryptocurrencies. De vervalsingen omvatten zowel identiteitsgegevens als foto’s, die vrij te kiezen waren. De documenten werden voornamelijk gebruikt voor fraude en witwassen.

Tijdens een reeks doorzoekingen in zeven Duitse deelstaten, uitgevoerd door ongeveer 300 federale politieagenten, werden belangrijke bewijzen verzameld. De autoriteiten troffen blanko identiteitskaarten, stempels, gravure-apparatuur en andere vervalsingsmaterialen aan. Ook werden waardevolle klantgegevens veiliggesteld, die nu verder onderzocht worden om andere klanten van de verdachte te identificeren. Het onderzoek wordt geleid door de centrale afdeling voor internetcriminaliteit van het openbaar ministerie in Frankfurt am Main. De verdachte bevindt zich momenteel in voorlopige hechtenis.

Meer dan 17.000 geheime gegevens blootgesteld op publieke GitLab repositories

Een beveiligingsonderzoeker heeft in totaal meer dan 17.000 blootgestelde geheime gegevens ontdekt in publieke repositories van GitLab, na het scannen van 5,6 miljoen repositories op GitLab Cloud. De onderzoeker, Luke Marshall, gebruikte de open-source tool TruffleHog om te zoeken naar gevoelige gegevens zoals API-sleutels, wachtwoorden en tokens in de code van de repositories.

GitLab, een platform voor softwareontwikkelaars, DevOps-teams en organisaties die werken met Continuous Integration/Continuous Deployment (CI/CD), werd in deze scan onder de loep genomen. Marshall voerde de scan uit met een aangepaste Python-script en een eenvoudige TruffleHog-opdracht, waarmee hij binnen 24 uur 5,6 miljoen unieke repositories analyseerde. De scan resulteerde in de identificatie van 17.430 blootgestelde geheime gegevens, waarvan de meerderheid bestond uit Google Cloud Platform (GCP)-referenties, gevolgd door sleutels voor MongoDB, Telegram-bot tokens en OpenAI-sleutels.

Dit incident is bijzonder relevant voor bedrijven en organisaties die GitLab gebruiken voor hun ontwikkelprocessen. De blootgestelde gegevens kwamen uit 2.804 unieke domeinen. Veel van deze geheimen waren relatief recent, maar sommige waren al sinds 2009 aanwezig en nog steeds actief.

Marshall nam verantwoorde maatregelen door de getroffen partijen te benaderen via geautomatiseerde meldingen. Hierdoor werd een groot aantal van de blootgestelde gegevens ingetrokken. Desondanks blijven sommige geheimen nog steeds zichtbaar in de publieke GitLab repositories. Deze ontdekking benadrukt de noodzaak voor bedrijven in Nederland en België om striktere beveiligingsmaatregelen te implementeren, met name voor het beheren van gevoelige gegevens in publieke code repositories.

Dit incident maakt duidelijk hoe belangrijk het is om gevoelige gegevens te controleren en te beschermen in de ontwikkelomgevingen die wereldwijd worden gebruikt, inclusief in Nederland en België. Organisaties die GitLab of andere platformen gebruiken, moeten waakzaam blijven en regelmatig controleren op mogelijke blootstelling van vertrouwelijke informatie.

Softwareprobleem bij Airbus-vliegtuigen: Impact op luchtverkeer in Nederland beperkt

Een softwareprobleem in Airbus-vliegtuigen, specifiek het type A320, heeft recent wereldwijd zorgen veroorzaakt. Dit probleem werd veroorzaakt door de impact van intense zonnestraling op de cockpitsystemen, wat leidde tot de noodzaak van een urgente software-update voor ongeveer 6000 toestellen. De update is bedoeld om storingen te voorkomen die de vluchtveiligheid kunnen beïnvloeden, een onderwerp dat ook relevant is voor de bredere discussie over de kwetsbaarheid van digitale systemen in kritieke infrastructuren.

In Nederland hebben de problemen geen invloed gehad op het luchtverkeer. Luchthavens zoals Schiphol hebben geen annuleringen gemeld voor vliegtuigen van het type A320, hoewel Airbus waarschuwde dat de software-update voor veel toestellen noodzakelijk was. Luchtvaartmaatschappijen zoals easyJet en Wizz Air hebben snel de benodigde updates doorgevoerd, wat aangeeft hoe digitale systemen, van luchtvaart tot andere infrastructuren, continu kwetsbaar kunnen zijn voor technische storingen en cyberrisico's.

Het incident werd aan het licht gebracht na een ernstige situatie waarbij een A320-vliegtuig tussen de VS en Mexico onverwacht hoogte verloor, wat leidde tot een noodlanding. Dit benadrukt de bredere risico's van technische kwetsbaarheden in systemen die cruciaal zijn voor de veiligheid van de luchtvaart, maar ook voor andere sectoren die afhankelijk zijn van digitale infrastructuren.

Thailand verbiedt links in sms en e-mail van overheidsinstellingen om oplichting te bestrijden

In Thailand heeft de overheid een belangrijke stap gezet in de strijd tegen online oplichting door alle overheidsinstellingen te verbieden sms-berichten en e-mails met links te versturen. Deze maatregel is bedoeld om criminelen die dergelijke links misbruiken om malware te verspreiden en burgers te misleiden, het leven moeilijker te maken. Thailand volgt hiermee de trend van andere landen die maatregelen nemen om de digitale veiligheid te verbeteren en oplichting via digitale kanalen te voorkomen.

De Thaise overheid is niet de enige die dergelijke maatregelen treft. In Nederland en België zijn soortgelijke campagnes en wetgeving in ontwikkeling om de veiligheid van digitale communicatie te waarborgen. Het is van cruciaal belang dat burgers in deze landen ook waakzaam blijven en zich bewust zijn van de risico's van frauduleuze berichten, vooral nu dergelijke misdrijven steeds meer wereldwijd worden gecoördineerd.

In Thailand is deze maatregel een uitbreiding van eerdere restricties, zoals het verbod van de Bank van Thailand op sms-berichten met links in juli 2025. Dit verbod geldt nu ook voor andere overheidsinstellingen. De overheid roept burgers op om berichten van officiële instanties zonder links als verdacht te beschouwen en te melden.

In Nederland en België blijft het een belangrijke taak voor zowel de overheid als bedrijven om maatregelen te treffen tegen de verspreiding van schadelijke berichten, waarbij ook technologieën zoals kunstmatige intelligentie en machine learning steeds vaker worden ingezet om oplichting te detecteren voordat het slachtoffers maakt.

Verkoop van AV- en EDR/XDR-killer tool en broncode op het darkweb

Op het dark web is recentelijk melding gemaakt van de vermeende verkoop van een geavanceerde tool die de werking van antivirussoftware (AV) en Endpoint Detection and Response (EDR)/Extended Detection and Response (XDR) systemen kan uitschakelen. Deze tool wordt gepromoot als een manier om de beveiligingssystemen van bedrijven en organisaties te omzeilen, wat de effectiviteit van de beveiligingsinfrastructuur ernstig kan ondermijnen. De broncode van de tool wordt eveneens aangeboden, wat betekent dat kwaadwillenden de mogelijkheid hebben om de software aan te passen en mogelijk nieuwe versies te ontwikkelen die nog moeilijker te detecteren zijn.

De verkoop van deze tool wijst op een toenemende dreiging van geavanceerde cyberaanvallen die gericht zijn op het uitschakelen van de eerste verdedigingslinie van bedrijven. Door antivirus- en detectiesystemen uit te schakelen, krijgen cybercriminelen de mogelijkheid om onopgemerkt binnen te dringen in netwerken en gevoelige informatie te stelen of verdere schade aan te richten. Dit type malware is bijzonder gevaarlijk voor organisaties die afhankelijk zijn van EDR/XDR-systemen om aanvallen in een vroeg stadium te detecteren en te stoppen.

Deze ontwikkeling benadrukt het voortdurende risico van geavanceerde dreigingen en de voortdurende strijd tussen cybersecurity-experts en cybercriminelen. De verkoop van dergelijke tools onderstreept de noodzaak voor organisaties om hun beveiligingsmaatregelen voortdurend bij te werken en te versterken om te voorkomen dat ze het slachtoffer worden van deze steeds geavanceerdere aanvallen.