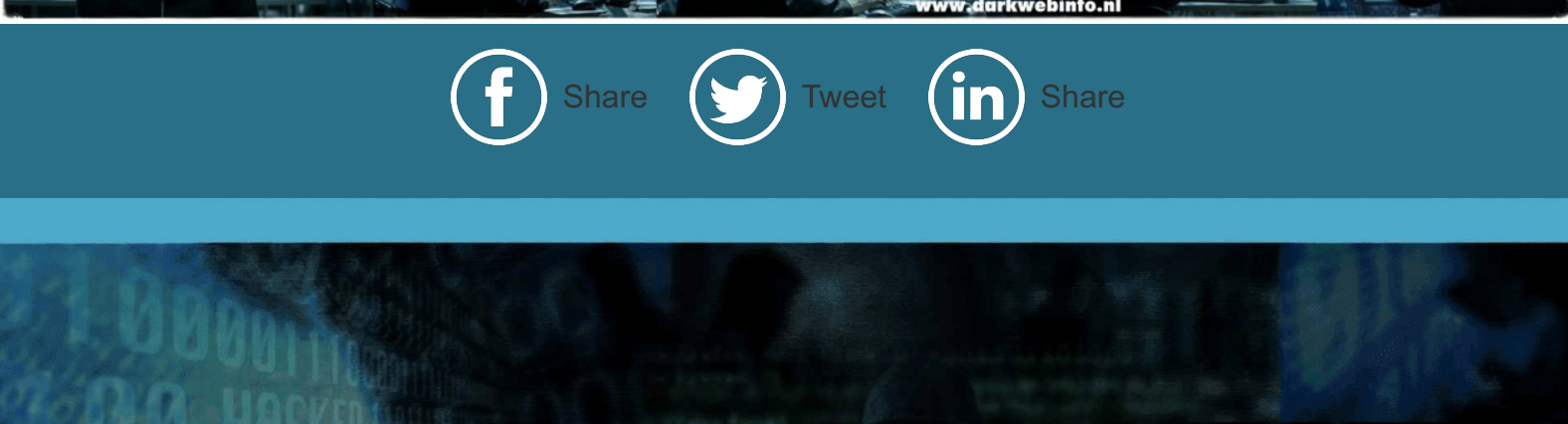


Nieuwsbrief 81 (week 47-2019) #CCINL |
www.cybercrimeinfo.nl



Share Tweet Share

74% is nog altijd onvoldoende voorbereid op cyberincidenten

Ruim de helft (55%) van alle MKB-organisaties is het afgelopen jaar een of meermaals slachtoffer geworden van cybercrime

Het is inmiddels niet meer de vraag of u een keer geraakt wordt door cybercrime, maar wanneer!

#CCINL | www.cybercrimeinfo.nl

Het is inmiddels niet meer de vraag of u een keer geraakt wordt door cybercrime, maar wanneer

Ruim de helft (55%) van alle MKB-organisaties is het afgelopen jaar een of meermaals slachtoffer geworden van cybercrime. Grote multinationals lopen nog altijd het meeste risico; 74% van de bedrijven met meer dan 1.000 werknemers kreeg te maken met digitale aanvallen. Slecht 10% scoort voldoende...

[LEES MEER >>](#)

Stijging internetoplichting

De politie heeft dit jaar 200 malafide webshops gesloten. Dat heeft Gijs van der Linden, teamleider van het Landelijk Meldpunt Internetoplichting (LMIO) van de politie bekendgemaakt in de uitzending van Radar. Daarnaast kon Van der Linden melden dat het aantal aangiftes over online oplichting met 7% is toegenomen tot een totaal van 47.000...

[LEES MEER >>](#)

Minstens 10 miljoen mensen potentieel doelwit van cyberaanvallen

"Dit is nog maar het topje van de ijsberg want we hebben in dit onderzoek alleen getoeken hoe kwetsbaar deze systemen zijn voor digitale inbreken via internetbrowsers"

#CCINL | www.cybercrimeinfo.nl

Minstens 10 miljoen mensen potentieel doelwit van cyberaanvallen

Het beheer van gebouwen wordt steeds verder geautomatiseerd, waarbij de systemen die worden gebruikt voor het bedienen van bijvoorbeeld alarmsystemen, stroomvoorziening, toegangsdeuren en -poorten, ventilatie of schuifdeuren steeds vaker zijn verbonden met internet. Doordat er te weinig aandacht is voor de digitale beveiliging, worden de systemen kwetsbaarder voor cyberaanvallen, terwijl de mogelijke impact van zulke aanvallen toeneemt...

[LEES MEER >>](#)

Bestandloze malware "Campagnes zonder infectie zijn moeilijk te detecteren"

Niet zoals criminelen kunnen worden gepakt door vingerafdrukken of DNA op de plaats delict, laten hackers ook sporen achter op geïnfecteerde systemen. Om het bewijs van hun aanvallen te verbloemen, hebben cybercriminelen bestandloze malware ontwikkeld. Deze schadelijke softwarevariant bestaat slechts als een artefact op het computergeheugen. De infectie of malware plaatst geen uitvoerbare bestanden op de harde schijf van het geïnfecteerde systeem om de detectie van de aanval zo lang mogelijk te verbergen...

[LEES MEER >>](#)

Aanvallers blijven gebruikmaken van meer sociale engineering en verfijsing

Miljoenen berichten met kwaadaardige URL's of bijlagen werden afgeleverd

#CCINL | www.cybercrimeinfo.nl

Aanvallers blijven gebruikmaken van meer sociale engineering en verfijsing

Ondanks een afwezigheid van bijna vier maanden, was de terugkeer van 'Emotet' in de laatste twee weken van september goed voor bijna 12 procent van alle kwaadaardige e-mailvoorbeelden in het derde kwartaal, waardoor miljoenen berichten met kwaadaardige URL's of bijlagen werden afgeleverd, vond Proofpoint...

[LEES MEER >>](#)

Week 47-2019

Extra controle na datalek Stichting Vecht
Datalek Busch
Honderden datalekken bij DWW en SVB
Incident databank e-mailadressen gemeente

#CCINL | www.cybercrimeinfo.nl

Datalek overzicht week 47-2019

[WEEK OVERZICHT >>](#)

Week 47-2019

ABN-AMRO
Albert Heijl

#CCINL | www.cybercrimeinfo.nl

PSV-cybercrime Phishing Smishing Vishing overzicht week 47-2019

[WEEK OVERZICHT >>](#)

Gezochte Personen

Culemborg - Jongeman fraudeert met persoonlijke gegevens
Zaaknummer: 2019441901
Datum delict: 03-10-2019
Plaats delict: Culemborg



Gezocht Persoon Cybercrime

#CCINL | www.cybercrimeinfo.nl

Culemborg - Jongeman fraudeert met persoonlijke gegevens

Zaaknummer: 2019441901

Datum delict: 03-10-2019

Plaats delict: Culemborg

Op 3 oktober 2019 wordt een pakketje met daarin een smartphone afgeleverd bij een woning aan de Nachtegaallaan in Culemborg. Dit betreft echter geen bestelling die de bewoners hebben gedaan. Op 4 oktober 2019 verschijnt dan een pakketje op de deur en zegt de hof van de koeriersdienst is. Hij 'komt' het pakketje ophalen omdat er een fout is gemaakt'. De bewoners hebben direct door dat het een oplichter is. De jongeman weet echter de benen te nemen...

[LEES MEER >>](#)

Dark Web

Darkweb Monitor als een service

Vanaf november 2019 zijn ongeveer 150.000 Dark Web-domeinen ontdekt waarvan bijna 10.000 services actief zijn en illegale goederen of services aanbieden

#CCINL | www.cybercrimeinfo.nl

Darkweb Monitor als een service

De Nederlandse Organisatie voor Toegepast Wetenschappelijk Onderzoek (TNO) en het in Nederland en Singapore gevestigde bedrijf CyberDevOps (CDO) zijn overeengekomen om Dark Web Monitor als een service te licentiëren. TNO en CDO delen een ambitie om cyberspace en ons digitale leven veiliger en veiliger te maken. Volgens de voorwaarden van de licentieovereenkomst zal CDO de Dark Web Monitor-service leveren aan een exclusief aanbod van wetshandhavinginstanties, beveiligingsorganisaties en bedrijven...

[LEES MEER >>](#)

Als eerste op de hoogte van Cybercrime nieuws?

U kunt zich inschrijven voor de automatische berichten service van Messenger, zo krijgt u ook als eerste de berichten van #CCINL | www.cybercrimeinfo.nl

Als eerste op de hoogte [Klik hier >>](#)

Tik vervolgens in de balk chatbericht het woord "ja" om de berichten automatisch te ontvangen.

Wat is? Cybercrime

Wat is Cybercrime en hoe goed is uw kennis? (Quiz)

Cybercrime is criminaliteit met ICT (Informatie- en Communicatie Technologie) als middel en doelwit, waarbij cybercriminelen inbreken op bijvoorbeeld een computer, telefoon of het complete netwerk van een organisatie. De motieven van cybercriminelen lopen uiteen. Veelal is dit om een grote hoeveelheid geld buit te maken of om een bedrijf schade aan te brengen. De impact is over het algemeen enorm...

[DOE DE QUIZ \(10 vragen\) >>](#)

Stop Cybercrime

Cybercrime tegenmaatregelen

2. Gebruik sterke wachtwoorden

Het gebruiken van een moeilijk te raden wachtwoord is belangrijk, vooral bij cruciale systemen zoals DigiD of uw wifi netwerk. Gebruik daarnaast voor elke dienst een uniek wachtwoord. Hiervoor kunt u gebruik maken van een wachtwoordmanager, die unieke wachtwoorden kan genereren en opslaan. Waar mogelijk gebruik tweestaps-verificatie om uw account extra te beschermen...

[LEES MEER >>](#)

11 Gouden Tips TIP 2

Schrijvers CCINL

SCHRIJVER BiG'r

#CCINL | www.cybercrimeinfo.nl

#CCINL Nieuwe artikel schrijver

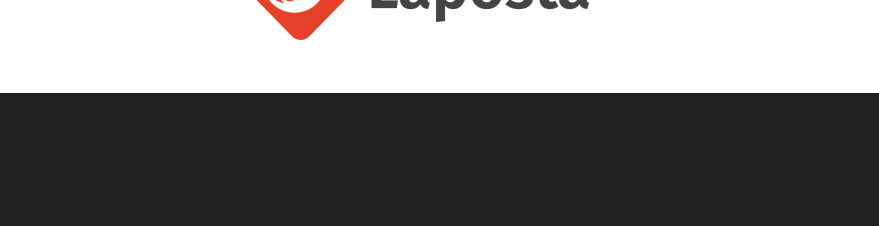
Met genoegen stel ik jullie onze 'Nieuwe' schrijver voor bij #CCINL | www.cybercrimeinfo.nl **BiG'r**

[WIE IS BiG'r >>](#)

Op de hoogte blijven over Cybercrime?

Wekelijks een nieuwsbrief ontvangen?

Schrijf je dan "hier" in.



Nieuwsbrief #CCINL | Cybercrimeinfo.nl

[Nieuwsbrief gemist?](#)

Nieuwsbrief Archief

Nog niet ingeschreven voor de wekelijkse nieuwsbrief?

Dat kan hieronder. Elke zondag of uiterlijk op maandag ontvang je dan de nieuwsbrief van #CCINL | www.cybercrimeinfo.nl

Zo blijf je altijd op de hoogte van het nieuws over Cybercrime en Darkweb...

Inschrijven wekelijkse nieuwsbrief [Klik hier >>](#)

Beste ambassadeurs van deze website

[Klik hier >>](#)

Deze e-mail is verzonden aan {{email}}. • Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich [hier afmelden](#). • U kunt ook uw [gegevens inzien en wijzigen](#). • Voor een goede ontvangst voegt u info@cybercrimeinfo.nl toe aan uw adresboek.

