CENTRE FOR
CYBER SECURITY
BELGIUM

Quel a été l'impact de la crise sanitaire sur le cyber-espace (belge) ?

Security Forum

13/10/2020

Phédra Clouner

Deputy Director

Agenda

- Le CCB… mais qu'est-ce?
- Crise sanitaire-crise cyber?
  - L'état de la menace
    - En temps normal
    - En période Covid-19
    - Et le télétravail? Opportunités et challenges
- Comment se protéger contre la cyber menace: en temps normal (et en temps de crise sanitaire)
  - Conseils et outils

Qui sommes-nous ? CCB ? CERT.be ?

FCCU ? = Federal Computer Crime Unit (police fédérale)

Vision

Faire de la Belgique l'un des pays les moins cybervulnérables d'Europe d'ici fin 2023

Base légale

- A.R. 10/10/2014

Contribuer à la construction d'un Internet plus sûr et plus sécurisé

Créer une politique nationale et des aptitudes en collaboration avec des acteurs existants

Politiques belges & coordination

Art. 3. Als nationale autoriteit heeft het CCB als opdracht :

1° opvolgen en coördineren van en toezien op de uitvoering van het Belgisch beleid ter zake;

2° vanuit een geïntegreerde en gecentraliseerde aanpak de verschillende projecten op het vlak van cyberveiligheid beheren;

3° de coördinatie verzekeren tussen de betrokken diensten en overheden, en de publieke overheden en de private of wetenschappelijke sector;

4° formuleren van voorstellen tot aanpassing van het regelgevend kader op het vlak van cyberveiligheid;

5° in samenwerking met het Coördinatie- en Crisiscentrum van de regering, het crisisbeheer bij cyberincidenten verzekeren;

6° opstellen, verspreiden en toezien op de uitvoering van standaarden, richtlijnen en veiligheidsnormen voor de verschillende informatiesystemen van de administraties en publieke instellingen;

7° coördineren van de Belgische vertegenwoordiging in internationale fora voor cyberveiligheid, van de opvolging van internationale verplichtingen en van voorstellen van het nationale standpunt op dit vlak;

8° coördineren van de evaluatie en certificatie van de veiligheid van informatie- en communicatiesystemen;

9° informeren en sensibiliseren van gebruikers van informatie- en communicatiesystemen.

Art. 3. Le CCB, au titre d'autorité nationale, a pour mission de :

1° superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en la matière;

2° gérer par une approche intégrée et centralisée les différents projets relatif à la cybersécurité;

3° assurer la coordination entre les services et autorités concernés mais aussi entre autorités publiques et le secteur privé ou le monde scientifique;

4° formuler des propositions pour l'adaptation du cadre légal et réglementaire en matière de cybersécurité;

5° assurer la gestion de crise en cas de cyberincidents, en coopération avec le Centre de coordination et de crise du gouvernement;

6° élaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes de sécurité pour les différents types de système informatique des administrations et organismes publics;

7° coordonner la représentation belge aux forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière;

8° coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication;

9° informer et sensibiliser les utilisateurs des systèmes d'information et de communication.

01

Quels types de cybermenace ?

Nous aimons les nouvelles technologies (encore plus en période de crise sanitaire!)

- Elles sont omniprésentes
- La digitalisation est omniprésente
- Elles facilitent notre vie quotidienne et ont sauvé l'économie Belge
  - TELETRAVAIL!!!!
  - Objets connectés-IOT
  - Services de cloud
  - Chat-bot
  - Réseaux sociaux
  - Big data
  - Blockchain
- Mais sont-elles sécurisées ?

ACTEURS DE LA MENACE

ET… Certains Etats…

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	→	1. Malware	→	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	→	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	→	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	→	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	→	10. Physical manipulation/ damage/ theft/loss	→	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Attaques fréquentes

- Phishing, Smishing, Vishing (‘Hameçonnage’ global, par sms ou par téléphone) *
- Distributed Denial Of Service Attack (DDOS) (‘attaque par déni de service’) *
- Watering hole (‘Attaque de point d’eau’)
- Ransomware (‘Rançongiciel’) *
- Fraude au CEO
- Advanced Persistent Threat (APT)

Phishing

Phishing

NL | FR | EN | DE

Contact | Actualités | Lettre d'information | Recherche avancée .be

Service public fédéral
Emploi, Travail et
Concertation sociale

Chercher: dans Actualités dans tout le site

GUIDE DE A À Z

THÈMES

- Réglementation du travail
- Contrats de travail
- Rémunération
- Non-discrimination et diversité
- Détachement
- Restructuration
- Concertation sociale
- Congés
- Bien-être au travail
- Emploi

Vous êtes ici: Page d'accueil > Actualités > **Attention aux faux e-mails usurpant la dénomination du SPF Emploi**

Attention aux faux e-mails usurpant la dénomination du SPF Emploi

26-07-2019 ▪ Le SPF Emploi a reçu plusieurs messages de personnes qui ont reçu un faux e-mail envoyé (de l'adresse spfemploi@outlook.be) par une certaine Mélanie DUMORTIER , chef du Service public fédéral Emploi, Travail et Concertation sociale. Cette personne n'existe pas et derrière ce mail se cachent des escrocs qui utilisent frauduleusement la dénomination de notre institution.

Il s'agit d'une tentative de phishing demandant de renvoyer des documents personnels, afin de vous escroquer (hameçonnage de données à caractère personnel pour souscrire frauduleusement à des crédits). Si vous recevez un e-mail de cet expéditeur, n'y répondez surtout pas et signalez-le à : suspect@safeonweb.be !

Antwoord aan: Federale Overheidsdienst Financiën <info@belastingdienst-fod.email>

Federale
Overheidsdienst
FINANCIEN

Geachte Debiteur,

We hebben helaas nog geen bedrag mogen ontvangen van uw Belastingaangifte van 2019.

Op **22 April 2020** zal de gerechtsdeurwaarder overgaan tot conservatoir beslag.

U kunt de beslagprocedure voorkomen door direct het gehele bedrag te voldoen

Wij verzoeken u dan ook vriendelijk om het openstaande bedrag
van € 136,21 voor **Woensdag 22 April** over te schrijven via het hieronder aangegeven knop.

KENMERK: M837281977
BEDRAG: € 136,21
TE VOLDOEN VOOR: Woensdag 22 April 2020

Voorkom Beslag

ROYAL BANK of NIGERIA
I have emailed everyone I can possibly find, my Prince, but no-one wants to help you move your money.
AGENT-X COMICS
WWW.AGENT-X.COM.AU

UW PAKKET BE3428632-19 IS ONDERWEG

bpost

UW PAKKET BE3428632-19 IS ONDERWEG

STATUS:
IN BEHANDELING - DISTRIBUTIE CENTRUM BRUSSEL

€4.95 VERZENDKOSTEN ZIJN NIET BETAALD

LEVERING VINDT PLAATS NA BETALING

BETAAL VERZENDKOSTEN

bpost

Smishing

Belangrijk! Het ticket van je vorige aankoop bij Colruyt werd geselecteerd op onze Jubileumtrekking. Je kunt nu je prijs verzamelen: http://g3h.us/HxR7m

Belfius

Uw huidige bankkaart zal binnenkort niet meer bruikbaar zijn. Wij vragen u daarom om uw nieuwe bankkaart
zo snel mogelijk aan te vragen. Klik op de link voor meer informatie. belfius.be.bmmndn.site/vervangen

ING

Vanwege een of meerdere ongebruikelijke inlogpogin(en) is uw rekening tijdelijk beperkt. verifieer uw account nu: ingbe-service.info

Beste Telenet Klant,

Je bent gekozen als winnaar van :
- Apple iPhone Xs
- Samsung Galaxy S10
- Apple Watch

Let op! Het aantal cadeau's is beperkt

Klik op OK om verder te gaan!

IP : 213.251.119.206

Gebruikersreferentie : 6241

Sluit

Distributed Denial Of Service Attack (DDOS)

BOTNETS

Forte augmentation des volumes par les botnets d'objets connectés à Internet. The Internet of Things (IoT)

WATERING HOLE ATTACKS

1. Attacker profiles victims and the kind of websites they go to.

2. Attacker then tests these websites for vulnerabilities.

3. When the attacker finds a website that he can compromise he then injects the JavaScript or HTML redirecting the victim to a separate site hosting the exploit code for the chosen vulnerability.

Site hosting exploit code

4. The compromised website is now "waiting" to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.

Symantec

Ransomware – Cryptoware

CryptoLocker

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on

1/6/2015 1:11:47 PM

Time left

71:52:21

Checking wallet..

Received: 0.00 BTC

Show files | Pay with Bitcoin

(Souvenez-vous du ransomware WannaCry 12/5/2017)

APT

- Qu'est-ce que c'est ?
  - Un logiciel malveillant complexe
  - Difficile à détecter – les protections traditionnelles (Firewall, Anti-Virus, IDS …) sont inopérantes.
  - Souvent développé à la carte pour une victime spécifique ou un petit groupe de victimes.
  - Contrôlé par une équipe dotée de ressources considérables.

- Objectif ?
  - Espionnage soutenu par des États (services de renseignement)
    - Exfiltration des données
    - Observation de la victime
    - Intégration de passages secrets dans des produits
    - Fourniture d'une présence permanente
  - Espionnage économique et scientifique
    - Organisation criminelle
  - Gains financiers :
  - Perturbation d'un État
  - Désinformation
  - Cyberguerre
  - Cyberterrorisme

Cyber-menaces et COVID-19

- Cibles
  - Secteur de la santé
    - Centres de recherche essentiellement, espionnage (vaccins) (WW)
  - Institutions financières
  - Entités gouvernementales
  - Groupes logistiques
- Surtout en Q1. pas d'augmentation en Q2 (autres actualités, autres sujets cf « black lives matter »)
- Familles de malwares utilisant le thème COVID-19 comme un leurre (ex Ursnif)
- Le site « info-coronavirus.be » a été considéré comme un site de phishing par certaines initiatives anti-phishing--> intervention du CCB (Be)
- Diverses attaques sponsorisées par des Etats utilisant des mails de phishing pour installer des malwares
- Arrestation de deux personnes à Amsterdam ayant lancé une campagne de phishing au nom d'ING (Be)
- Attaque DDOS contre un hôpital à Bruges, et un hopital à Ostende (Be)
- Ransomwares: augmentation en Belgique et dans le monde (cryptage+divulgation). Ex: MAZE (centre de recherche)
- Vulnérabilités identifiées dans certains produits (dont des VPN's)→ danger important en raison du télétravail généralisé!!!

Malwares et COVID-19

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/covid-19-malware-makes-hay-during-a-pandemic/

COVID-19

- Augmentation du phishing
  - Phishing ➔ 600% (UN)
  - Scams (personal protective equipment)

- On change la cible!

BOB WORKS FROM HOME TO ESCAPE THE DISTRACTION OF OFFICE CHIT CHAT.

COVID-19

- On change la cible ➔ CONSEQUENCES
  1. Les thèmes de phishing ont changé
  2. Les criminels exploitent les vulnérabilités des produits permettant le travail en remote (VPN's , RDP, etc)
  3. Malware android à travers des app ayant pour thème le COVID-19
     - Vol des données d'authentification
     - Verrouillage, cryptage ou effacement de l'appareil pour obtenir une rançon
     - Keylogging: Le logiciel enregistre toutes les touches saisies au clavier
     - Adware: logiciel publicitaire
     - Financier : Voler les identifiants bancaires
     - Espionner en écoutant, en filmant, en prenant des captures d'écran

LE PHISHING! (encore lui!!!!)

Phishing mails sent to suspicious@safeonweb.be

COVID-19 Related Phishing Emails in Belgium, Source: CCB

COVID-19 Related Phishing Emails in Belgium, Source: CCB

	Week 14	Week 15	Week 16	Week 17	Week 18	Week 19	Week 20	Week 21	Week 22	Week 23	Week 24	Week 25	Week 26
Corona	60	59	43	62	55	43	32	16	16	9	20	7	4
COVID	32	29	45	35	33	44	40	21	9	5	5	0	0
Masker/masque/mask	50	45	113	238	171	93	46	31	19	31	6	1	5
kapje	0	0	0	0	0	45	24	9	6	4	1	3	0
desinfectie/disinfection	0	0	0	0	0	8	14	6	3	6	6	0	1

20/4

1/6

Van: SafeMask Promotion <info@jdnserver.nl>
Datum: 5 maart 2020 om 18:03:15 CET
Aan: [redacted]
Onderwerp: ⚠ **Coronavirus warning: This mask adds an extra layer of protection...**
Antwoord aan: info@great.speedskincare.com

View Offer

The best-selling SafeMask!

SafeMask keeps you and your loved ones safe, even during the worst air pollution ocurrences and during the yearly outbreaks of several dangerous viruses.

We also recommend you to take advantage of the very attractive multiple order discounts that is offering. Why not get one for your loved ones or one for your friends? Take advantage now, since these discounts won't last forever.

Click here to buy SafeMask - 50% Off & Free Shipping!

If you'd prefer not to receive future emails, Unsubscribe Here.
23638 W. Lyons Avenue #468 SC Newhall, CA 91321

RODE KRUIS
Wereldwijd in actie tegen het coronavirus, wegens het aanhoudende coronavirus vragen wij u om een eenmalige donatie om verdere verspreiding te voorkomen en hulp te verlenen via:
https://rodekruis.be.donaties.site/pay/DR5JM9utn4

L'arnaque par sextorsion version

safeonweb.be/fr/actualite/lamaque-par-sextorsion-version-covid-19

coronavirus/

Subject: [YOUR NAME] : [YOUR PASSWORD]

I know every dirty little secret about your life. To prove my point, tell me, does [REDACTED]] ring any bell to you? It was one of your passwords.

What do I know about you?

To start with, I know all of your passwords. I am aware of your whereabouts, what you eat, with whom you talk, every little thing you do in a day.

What am I capable of doing?

If I want, I could even infect your whole family with the CoronaVirus, reveal all of your secrets. There are countless things I can do.

What should you do?

You need to pay me $4000. You'll make the payment via Bitcoin to the below-mentioned address. If you don't know how to do this, search 'how to buy bitcoin' in Google.
Bitcoin Address:
[REDACTED]
(It is cAsE sensitive, so copy and paste it)

You have 24 hours to make the payment. I have a unique pixel within this email message, and right now, I know that you have read this email.

If I do not get the payment:

I will infect every member of your family with the CoronaVirus. No matter how smart you are, believe me, if I want to affect, I can. I will also go ahead and reveal your secrets. I will completely ruin your life.

Nonetheless, if I do get paid, I will erase every little information I have about you immediately. You will never hear from me again. It is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Nikita

naked security by SOPHOS

Vous avez reçu un message de ce type ? Pas de panique !

FRA 19:26 12-07-20

Text Message
Today 3:45 PM
Someone who came in contact with you tested positive or has shown symptoms for COVID-19 & recommends you self-isolate/get tested. More at COVID-19anon.com/alert

Cibles gouvernementales

- Mail de phishing au nom du SPF intérieur (communes NL)
- Informations de comptes liés à la santé publique et fedasil ont été divulguées (via malware)

Nieuw bericht in uw eBox

Van: "My eBox" <info@csam-administratie.email>

Aan: [redacted]

my e-box — Nieuw bericht in uw beveiligde elektronische brievenbus

Geachte Heer/Mevrouw,

U heeft een nieuw bericht ontvangen van FOD Financiën in uw eBox.
'Bekijk hoe u in aanmerking komt voor een Corona Crisis compensatie.'
U kan dit bericht inkijken tot 30/06/2020.

Bekijk dit bericht via My eBox :

Ga naar My eBox

Het eBox team

Heeft u vragen of opmerkingen over dit bericht ? Contacteer ons

© 2020 BOSA DT | Gebruiksvoorwaarden | Privacy .be

Et le télétravail?

- La plupart des organisations n'étaient pas préparées à un mode « full télétravail »
  - …. Les employés non plus!
  - Certains employés utilisaient leur propre matériel
  - Certains n'utilisaient pas de VPN pour sécuriser leur connexion
  - Difficile de traiter des informations sensibles quand la frontière entre vie pro et vié privée devient floue
  - La plupart des organisations pensaient avant tout à survivre et se concentraient sur leur core business
    - La sécurité n'étaient pas au centre des préoccupations
  - La vidéo-conférence est devenue la norme… mais elle n'était pas toujours utilisée de manière adéquate!

We Help our Hospitals!

- https://wehelpourhospitals.be/
- Partenariat Public-privé pour protéger les… hôpitaux!
- Cyber réserve
- plusieurs entreprises et experts indépendants spécialisés dans la cybersécurité ont décidé de mettre leur expertise à titre bénévole à la disposition des hôpitaux
  - 19 entreprises
  - Plusieurs dizaines de volontaires
- Conseils et aide en cas de cyber incidents
- Réflexion sur l'extension du concept

02

Comment se protéger ? (Ce n’est pas si compliqué !)

Pourquoi me protéger ?

- Parce que les cybercriminels exploitent les informations publiées sur les réseaux sociaux pour cibler leurs victimes
- Soyez prudents lorsque vous parlez de votre travail !

Les conseils du CCB en matière de télétravail

- https://www.safeonweb.be/fr/blog/teletravail-securise-volet-1-un-reseau-bien-securise
- Un réseau bien sécurisé
  - Installation d'un VPN
  - Routeur: modifiez votre nom de réseau (SSID) : pas votre adresse ^^
  - Routeur: modifiez vos mots de passe réseau
  - Routeur: protection WPA2 (cryptage)
  - Routeur: mises à jour
  - Activez votre pare-feu et utilisez un anti-virus
  - Désactivez le WPS (connexion plus facile sans MDP)
  - Créez un réseau hôte (réseau Wifi distinct du réseau personnel)
  - Utilisez un câble éthernet
- Un environnement de travail sûr
  - Verrouillez votre ordinateur
  - Oubliez le post-it pour vos mots de passe
  - Attention si vous devez avoir une conversation confidentielle
  - Cryptez les données de votre PC (bitlocker MS –FileVault Mac)
  - Eteignez votre ordinateur tous les soirs (MàJ)
  - Utilisez des outils de communication sécurisés pur les infos confidentielles (Threema-Telegram-etc)
- Reconnaissez les messages de phishing!!!!!!!

NO MORE RANSOM!

English

Crypto Sheriff | Ransomware: Q&A | Prevention Advice | Decryption Tools | Report a Crime | Partners | About the Project

New decryptor for **MacRansom** available, please click **here**.

NEED HELP unlocking your digital life without paying your attackers*?

YES NO

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.

BAD NEWS

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.

GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

https://www.nomoreransom.org

Recommandations SafeOnWeb

1. Effectuer un scan de son ordinateur et utiliser un logiciel antivirus

2. Veiller à la mise à jour de vos programmes

3. Faire des back-ups (cloud)

4. Reconnaître le phishing

5. Utiliser des mots de passe sûrs et

2 FA authentication (oublier le post it ;-))- Sujet de l

Campagne 2020!!!

Reconnaître le phishing

Mince ! Vous avez cliqué ?!

- Le message a été transmis à vos amis ?
  - Mettez-les en garde !
- Vous avez communiqué un mot de passe ?
  - Changez le mot de passe partout où vous l'utilisez
- Vous avez communiqué des coordonnées bancaires ?
  - Prévenez votre banque et Cardstop (070/344344, numéro à conserver dans les contacts)
- Un programme risque d'avoir été installé ?
  - Effectuez un scan antivirus
- Cela vous est arrivé au travail ?
  - Prévenez votre service informatique. Ils peuvent éviter que d'autres soient pris au piège ou qu'un virus continue à se propager.
- Supprimez le message.

Bravo ! Vous avez identifié un message suspect

- Transférez-le à suspect@safeonweb.be
- Le message vient d'une banque ou d'une organisation connue ?
  - Transférez-le à l'organisation ou la banque en question. Ils apprécient d'être mis au courant lorsque leur nom est exploité à des fins de phishing. Les banques ont une adresse e-mail spécifiquement dédiée : phishing@NOMDELABANQUE.be
- Vous avez reçu le message suspect sur votre adresse professionnelle ?
  - Transférez-le à votre service ICT. Une démarche est peut-être déjà prévue en interne.
- Supprimez le message

CCB.BELGIUM.BE

Guide de référence en cybersécurité

Guide de référence en cybersécurité

Take security measures / Manage access to your computers and networks

Basic | Advanced

Plan your cyber security

Manage risks for your most important assets

Take security measures

- Have a business continuity and an incident handling plan
- Manage access to your computers and networks
- Manage your key ICT assets
- Install antivirus protection
- Update all programs
- Back up all information
- Secure remote access
- Secure workstations and mobile devices
- Secure servers and network components
- Secure your website

Evaluate your actions

MANAGE ACCESS TO YOUR COMPUTERS AND NETWORKS

Just as you manage the physical security of your organization, you must manage information security. Do not leave your information accessible to everybody, at any time.

- Users are only authorized to access the information they need to perform their duties
- Immediately disable unused accounts
- Rights and privileges are managed by user groups
- Change all default passwords
- Passwords must be longer than 10 characters with a combination of character types and changed periodically or when there is any suspicion of compromise
- Enforce authentication and password rules
- Use only individual accounts and never share passwords
- Keep a limited and updated list of system administrator accounts
- No one works with administrator privileges for daily tasks

Webinaires

- https://ccb.belgium.be/fr/publication/webinaires-pour-les-organisations
- Public cible
  - Directeurs et gérants d'entreprise
  - Management
  - Personnel IT
- Durée : 10-30 minutes max.
- Conseils utiles et pratiques
- Basés sur les meilleures pratiques/ normes internationales/ ENISA/ etc
- Réalisés par des experts : Police/ secteur public (SPF Économie par exemple/ universitaires/ acteurs privés
- FR-NL
- Sujets
  - Sensibilisation
  - Fraude au CEO
  - Phishing
  - Ransomware
  - Mots de passe
  - Cybermenaces
  - Mises à jour
  - RGPD
  - Réponse aux incidents

Boîte à outils pour la cybersécurité

- Prête à l'emploi
- La sensibilisation renforce la cybersécurité !
- En collaboration avec la Cybersecurity Coalition
- Formation de base
- 3 sujets
  - Phishing
  - Social engineering
  - Mots de passe sûrs
- Contenu de la boîte à outils
  - E-mail pour les collaborateurs
  - Posters
  - Présentation pour une séance d'information
- www.cybersecuritycoalition.be

CYBER SECURITY COALITION.be

WWW.CERT.BE

NL FR DE EN

Other official information and services: www.belgium.be .be

CERT.be
The Federal Cyber Emergency Team

Search

About us | Report an incident | Advisories | News | Vacancies | Contact

Welcome to CERT.be

The federal Computer Emergency Response Team, or CERT.be for short, is the operational service of the Centre for Cyber Security Belgium (CCB). The task of CERT.be is to detect, observe and analyse online security problems, and to inform various target groups accordingly.

RECENT ADVICE AND WARNINGS

REMOTE ROOT CODE EXECUTION VULNERABILITY IN EXIM MTA
2019-09-06 16:30
CERT.be recommends to system administrators to patch your systems immediately if they are running Exim.

VULNERABILITY IN PULSE SECURE: PULSE CONNECT SECURE (PCS)
2019-08-27 12:56
CERT.be recommends all System administrators to upgrade their vulnerable Pulse Secure instances to version 9.1R1 and above.

BLUEKEEP: WINDOWS RDP REMOTE CODE EXECUTION VULNERABILITY V2
2019-08-14 10:33
CERT.be recommends administrators to update their Microsoft Windows systems with the latest available patches as soon as possible:

CENTRE FOR CYBER SECURITY BELGIUM

@Certbe

Des questions ?

Info@ccb.belgium.be