Safeonweb
@Work

EEN INITIATIEF VAN

CENTRE FOR CYBER SECURITY BELGIUM

CYBER FUNDAMENTALS

SMALL

Versie 2023-03-01

Centrum voor Cybersecurity België
Wetstraat 18
1000 Brussel
België

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

Inhoudsopgave

Inleiding

Het **CCB Cyberfundamentals Framework is** een reeks concrete maatregelen om:

- gegevens te beschermen,
- het risico van de meest voorkomende cyberaanvallen aanzienlijk verminderen,
- de cyberweerbaarheid van een organisatie vergroten.

Om in te spelen op de ernst van de bedreiging waaraan een organisatie is blootgesteld, worden naast het niveau **Small** 3 betrouwbaarheidsniveaus geboden: **Basis, Belangrijk en Essentieel** ("Basic", "Important" en "Essential"**)**.

Met het **startniveau Small kan** een organisatie een eerste beoordeling maken, waarbij de aspecten in verband met de interne ontwikkeling van applicaties buiten beschouwing worden gelaten.

Het startniveau Small is bedoeld voor micro-organisaties (behalve in een risicovolle omgeving) of organisaties met beperkte technische kennis.

Het raamwerk is een levend document en zal voortdurend worden bijgewerkt en verbeterd, rekening houdend met de feedback van belanghebbenden, het evoluerende risico van specifieke cyberbeveiligingsdreigingen, de beschikbaarheid van technische oplossingen en voortschrijdend inzicht.

1 BESCHERM ALLE LOGINS MET MULTIFACTOR AUTHENTICATIE

Gebruik waar mogelijk Multifactor Authenticatie.
Gebruik altijd Multifactor Authenticatie bij toegang op afstand

Richtlijnen

De meeste tools voor Multifactor Authenticatie combineren uw wachtwoord met dingen die u hebt (smartphone, badge, ID-kaart) of dingen die u bent (vingerafdruk). Het gebruik van meerdere elementen voor authenticatie vermindert het risico op hacken.

- Gebruik een pasvraag, een verzameling van ten minste drie willekeurige gemeenschappelijke woorden gecombineerd tot een zin die een zeer goede combinatie van onthoudbaarheid en veiligheid biedt.
  Als u kiest voor een typisch wachtwoord:
  - Maak het lang, met kleine letters en hoofdletters, eventueel ook cijfers en speciale tekens.
  - Vermijd voor de hand liggende, zoals "wachtwoord", reeksen letters of cijfers zoals "abc", getallen zoals "123".
  - Vermijd het gebruik van persoonlijke informatie die online te vinden is.
- Wanneer u wachtzinnen of wachtwoorden gebruikt
  - Gebruik ze niet elders opnieuw.
  - Wijzig het wachtwoord zodra het vermoeden ontstaat dat het gecompromitteerd is.
- Schakel Multifactor Authenticatie in. Er zijn veel MFA tools beschikbaar, het is het beste om een MFA tool te kiezen die verschillende authenticatie opties biedt.
  MFA is van het grootste belang voor internetgerichte systemen zoals bijvoorbeeld toegang op afstand. Toegang op afstand kan worden gerealiseerd via bijvoorbeeld VPN (Virtual Private Network), RDP (Remote Desktop Protocol).

2 INSTALLEER ONMIDDELLIJK ALLE BEVEILIGINGSUPDATES

Implementeer beveiligingsupdates/patches voor al uw software zodra deze beschikbaar zijn.

Richtlijnen

- Nu ontwikkelaars de strijd aangaan met cybercriminelen om hun software veiliger te maken en minder kwetsbaar voor de nieuwste aanvallen, is zo snel mogelijk patchen de sleutel tot meer cyberveiligheid.
- Denk aan de volgende maatregelen:
  - Beperk u tot het installeren van alleen die toepassingen (besturingssystemen, firmware of plugins) die u nodig hebt om uw organisatie te laten draaien.
  - Installeer alleen door de leverancier ondersteunde versies van software die u wilt gebruiken.
  - Automatiseer het updateproces zoveel mogelijk door automatische updates als standaardinstelling in te stellen op de besturingssystemen van uw eindpunten.
  - Er zijn producten die uw systeem kunnen scannen en u verwittigen wanneer er een update is voor een toepassing die u hebt geïnstalleerd. Als u een van deze producten gebruikt, zorg er dan voor dat het op updates controleert voor elke toepassing die u gebruikt. Als u deze producten niet gebruikt, wijs dan elke maand een dag aan om de beschikbaarheid van nieuwe patches te controleren en deze te installeren.

3 INSTALLEER ANTIVIRUS

Implementeer een antivirusoplossing op alle soorten apparaten en houd deze up-to-date om de continue doeltreffendheid ervan te garanderen.

Richtlijnen

Zelfs met de beste voorzorgsmaatregelen kunt u te maken krijgen met een virus of malware. Een anti-malware software is een tweede barrière die u beschermt tegen de impact van cyberincidenten.

- De geselecteerde anti-malware software moet bescherming bieden tegen alle soorten malware zoals virussen, spyware, adware en rootkits.
- Het is aanbevolen om de anti-malware software in te stellen om minstens dagelijks (of wanneer beschikbaar in "real-time") automatisch te controleren op updates, en dan spoedig een volledige scan uit te voeren. Wanneer meerdere apparaten (thuiscomputers, laptops, tablets...) worden gebruikt, moet op al deze apparaten anti-malware software worden geïnstalleerd en bijgewerkt.
- Als preventieve maatregel moeten de volgende regels worden toegepast:
  - Deel geen USB-drives of externe harde schijven tussen persoonlijke en zakelijke computers of apparaten.
  - Sluit geen onbekende / niet-vertrouwde hardware aan op uw systeem of netwerk en plaats geen onbekende externe USB-stick. Deze apparaten kunnen malware bevatten. Schakel de AutoRun-functie voor draagbare schijven (USB, optische...) op uw bedrijfscomputers uit om te voorkomen dat dergelijke kwaadaardige programma's op uw systemen worden geïnstalleerd.
  - Installeer geen illegale software, want die kan malware bevatten.

4 BEVEILIG UW NETWERK

Bescherm uw netwerk door een firewall te installeren.
Bescherm gegevens op het netwerk waartoe toegang wordt verkregen via WiFi met behulp van draadloze versleutelingsnormen.
Besteed specifieke aandacht aan de beveiliging van toegang op afstand .

Richtlijnen

- Deel je WIFI wachtwoorden met niemand.
- Indien nodig scheidt u uw WIFI-netwerk voor gasten/bezoekers van uw professionele netwerk.
- Tussen uw interne netwerk en het internet moeten firewalls worden geïnstalleerd en geconfigureerd. Dit kan een functie zijn van een (draadloos) toegangspunt/router, of het kan een functie zijn van een door de Internet Service Provider (ISP) geleverde router. De firewalls moeten worden geactiveerd en bijgewerkt. U kunt de dienstencatalogus van uw ISP raadplegen over de geleverde netwerkbeveiligingsdiensten.
  - Zorg ervoor dat het administratieve wachtwoord van uw firewall bij de installatie en daarna regelmatig wordt gewijzigd. Overweeg ook om de inloggegevens van de beheerder
  - Encryptie maakt uw elektronisch opgeslagen informatie onleesbaar voor iedereen die niet over het juiste wachtwoord of de juiste sleutel beschikt. Stel uw router in om ten minste WiFi Protected Access (WPA-2 of WPA-3 indien mogelijk) te gebruiken, met de Advanced Encryption Standard (AES) voor encryptie.

5 BACK-UP VAN UW GEGEVENS

Maak regelmatig automatische back-ups van uw informatie.
Zet wekelijks of om de paar weken een back-up OFF LINE (niet aangesloten op het netwerk).
Maak na de belangrijkste wijzigingen een back-up van uw systemen, zodat u ze gemakkelijker kunt herstellen.

Richtlijnen
Bedenk hoeveel u vertrouwt op uw organisatie kritische gegevens. Door back-ups te maken en te testen kunt u uw gegevens en ICT-systemen herstellen in geval van een groot cyberbeveiligingsincident (bijvoorbeeld een ransomware-aanval).
Enkele basisrichtsnoeren om te overwegen:

- Bepaal welke gegevens u moet back-uppen. Dit zijn de essentiële gegevens/informatie waar uw organisatie niet zonder kan.
- Bepaal de back-upfrequentie op basis van de hoeveelheid gegevens (bijgewerkt of gecreëerd) die na een storing verloren gaan of opnieuw moeten worden ingevoerd.
- Scheid back-up media van uw andere opslagsystemen. Een offline back-up is zeer belangrijk om de mogelijkheid te beperken dat uw back-up ook wordt versleuteld of gewist in geval van een hack.
- Test het terugzetten van de gegevens op regelmatige tijdstippen. Het is ook een basiscontrole of de back-upprocedure goed verloopt.

6 ADMINISTRATIERECHTEN

Zorg ervoor dat niemand werkt met beheerdersrechten voor dagelijkse taken.

Richtlijnen
Een beheerder heeft veel toegang tot uw systeem. Het beschermen van deze accounts is erg belangrijk omdat ze veel waarde hebben voor cybercriminelen. Overweeg de volgende principes om deze accounts te beschermen:

- Scheid beheerdersaccounts van gebruikersaccounts. Voor het dagelijkse werk volstaat een gebruikersaccount zonder beheerdersrechten.
- Multifactorauthenticatie vereisen voor alle toegang via beheerdersaccounts.

7 SLOTAANBEVELINGEN

Bescherm uw computers en mobiele apparaten fysiek tegen diefstal of oneigenlijk gebruik.

De toegang tot gebouwen, back-ups, servers en netwerkcomponenten beperken tot bevoegde personen.

Weet hoe en met wie u contact moet opnemen bij een cyberincident.

Richtlijnen

- Fysieke beveiliging en toegangsbeperking:
  - Fysieke beveiliging is de bescherming van personeel, hardware, software, netwerken en gegevens tegen fysieke acties en gebeurtenissen die uw organisatie ernstig verlies of schade kunnen berokkenen.
  - Er zijn betaalbaar geprijsde beheersystemen voor mobiele apparaten die een optie kunnen zijn als u veel gebruik maakt van mobiele apparaten. Het inschakelen van toepassingen zoals "Zoek mijn telefoon" op uw mobiele telefoons kan een eerste stap zijn.
  - Beheer strikt de sleutels voor toegang tot de gebouwen en de alarmcodes.
- In geval van een incident:
  - Bewaar een offline kopie (bv. offline harde schijf of laptop, papieren hardcopy, ...) van elk document dat u waarschijnlijk nodig zult hebben tijdens een cyberbeveiligingsincident of -crisis door de volgende vragen te beantwoorden:
    - Met wie moet ik contact opnemen in geval van een cyberincident?
    - Welke info heb ik nodig om met hen in contact te komen?
    - Welke info zullen ze vragen?
  - Zie ook onze aanbevelingen in de CCB Cyber Security Incident Management guide die een pragmatische aanpak biedt voor het omgaan met cyberbeveiligingsincidenten en als inspiratie kan dienen voor uw eigen incident response plan of draaiboek.

Disclaimer

Dit document en zijn bijlagen zijn opgesteld door het Centrum voor Cyberveiligheid België (CCB), een federale administratie opgericht bij koninklijk besluit van 10 oktober 2014 en onder het gezag van de eerste minister.

Dit document bevat technische informatie die oorspronkelijk in het Engels is geschreven. Deze informatie heeft betrekking op de beveiliging van netwerken en informatiesystemen is gericht tot IT-diensten die de Engelse termen van computertaal gebruiken. Een vertaling in het Nederlands, Frans of Duits van deze technische informatie is niettemin beschikbaar bij het CCB.

Het CCB aanvaardt **geen verantwoordelijkheid voor de inhoud** van dit document.
De verstrekte informatie:

- Is uitsluitend van algemene aard en zijn niet bedoeld om rekening te houden met alle bijzondere situaties.
- Is niet noodzakelijkerwijs volledig, nauwkeurig of op alle punten actueel.

Verantwoordelijke redacteur

Centrum voor Cyberveiligheid België
De heer De Bruycker, directeur-generaal
Wetstraat, 18
1000 Brussel

Juridisch depot

D/2023/14828/001