CENTRE FOR CYBERSECURITY BELGIUM

Richtlijn n° 1/2024 van 24 januari 2024

CCB richtlijn voor de verschillende informatiesystemen van de administraties en publieke instellingen

---

Het Centrum voor Cybersecurity België (CCB) dringt er bij de administraties en publieke instellingen op aan om zo snel als mogelijk tweestapsverificatie (2FA) te activeren op alle externe verbindingen met hun netwerken en systemen. Het is de verantwoordelijkheid van elke overheidsdienst om de dienstverlening te garanderen en de gegevens van de burger optimaal veilig te stellen. 2FA is een eenvoudige en haalbare inspanning die een wereld van verschil maakt voor de cyberveiligheid van de overheden.

Dagelijks wordt er in ons land een organisatie of bedrijf het slachtoffer van een ransomware-aanval of van afpersing na diefstal van gevoelige informatie. In 2023 deden 120 private en publieke organisaties een melding bij het CCB. Steden, gemeenten en andere overheidsdiensten blijven niet gespaard, leren ons de cyberaanvallen van het afgelopen jaar. Nochtans kunnen deze aanvallen vaak vermeden worden.

Volgens artikel 3, 6°, van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België heeft het CCB o.a. de opdracht om standaarden, richtlijnen en veiligheidsnormen voor de verschillende informatiesystemen van de administraties en publieke instellingen op te stellen, te verspreiden en toe te zien op de uitvoering van. Daarom vraagt het CCB de administraties en publieke instellingen de uitvoering van de volgende richtlijnen in het domein van de cyberveiligheid:

- **Installeer zo snel als mogelijk tweestapsverificatie**

Uit onze vaststellingen bij incidenten blijkt dat cybercriminelen vaak gebruik maken van gestolen logingegevens om hun aanval in te zetten. De beste manier om uw organisatie hier tegen te wapenen is gebruik maken van tweestapsverificatie (2FA) op alle verbindingen van buiten het bedrijf of de organisatie.
Meer info over de implementatie van 2FA: https://atwork.safeonweb.be/nl/MFA

- **Maak uw organisatie conform het CCB Cyber Fundamentals Framework**

Het CCB beschikt over een raamwerk, de zogenaamde Cyber Fundamentals, dat organisaties de weg wijst naar een gepaste cyberweerbaarheid. Alle administraties en publieke instellingen nodigen we uit om het gepaste niveau van Cyber Fundamentals te hanteren als veiligheidsnorm voor de organisatie. Het CCB stelt eveneens een eenvoudige tool beschikbaar om het gepaste niveau eenvoudig te kunnen bepalen.
Meer info over de Cyber Fundamentals Framework: https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

Centrum voor cyberveiligheid België
Onder het gezag van de Eerste minister
Wetstraat 18 - 1000 Brussels
www.ccb.belgium.be

- **Administraties en publieke instellingen laten zich niet afpersen**

Het CCB adviseert om ransomware-betalingen collectief aan te pakken en om het ransomware-bedrijfsmodel te ondermijnen en criminele activiteiten te verstoren. We zullen de afpersende acties van deze cybercriminelen niet tolereren.
Daarom raden we iedereen ten zeerste af om een ransomware-eis te betalen. Het betalen van losgeld aan ransomware-actoren:

- garandeert niet het einde van een incident, of de verwijdering van kwaadaardige software;
- moedigt criminelen aan om hun activiteiten voort te zetten en uit te breiden;
- voorziet criminele actoren van extra middelen;
- garandeert niet dat u uw gegevens terugkrijgt of dat ze niet publiek gemaakt worden.

Miguel De Bruycker
Directeur Generaal CCB