CENTRE FOR CYBERSECURITY BELGIUM

Stellungnahme n° 1/2024 vom 24. Januar 2024

Richtlinie des ZCB für die verschiedenen Informationssysteme von Verwaltungen und öffentlichen Einrichtungen

Das Zentrum für Cybersicherheit Belgien (ZCB) fordert Verwaltungen und öffentliche Einrichtungen auf, so bald wie möglich die Zwei-Faktor-Authentisierung (2FA) für alle externen Verbindungen zu ihren Netzwerken und Systemen zu aktivieren. Es liegt in der Verantwortung jeder öffentlichen Verwaltung, die Bereitstellung von Dienstleistungen und die optimale Sicherheit der Daten der Bürger zu gewährleisten. 2FA ist eine einfache und praktikable Maßnahme, die die Cybersicherheit von Behörden erheblich verbessern wird.

Täglich wird eine Organisation oder ein Unternehmen in unserem Land Opfer eines Ransomware-Angriffs oder einer Erpressung nach dem Diebstahl sensibler Daten. Im Jahr 2023 meldeten sich 120 private und öffentliche Organisationen beim ZCB. Städte, Gemeinden und andere öffentliche Dienste bleiben nicht verschont, wie uns die Cyberangriffe des letzten Jahres lehren. Allerdings können diese Angriffe oft vermieden werden.

Gemäß Artikel 3, 6°, des königlichen Erlasses vom 10. Oktober 2014 zur Einrichtung des Zentrums für Cybersicherheit Belgien (*Arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique*) umfasst der Auftrag des ZCB die Ausarbeitung, Verbreitung und Überwachung der Umsetzung von Standards, Richtlinien und Sicherheitsnormen für die verschiedenen Informationssysteme von Verwaltungen und öffentlichen Einrichtungen. Daher fordert das ZCB die Verwaltungen und öffentlichen Einrichtungen auf, die folgenden Richtlinien im Bereich der Cybersicherheit umzusetzen:

- **Schnellstmöglich Zwei-Faktor-Authentisierung installieren**

Unsere Beobachtungen von Vorfällen zeigen, dass Cyberkriminelle häufig gestohlene Anmeldedaten verwenden, um ihre Angriffe zu starten. Die beste Möglichkeit, Ihr Unternehmen dagegen zu wappnen, ist die Verwendung einer Zwei-Faktor-Authentisierung (2FA) für alle Verbindungen von außerhalb des Unternehmens oder der Organisation.
Weitere Informationen zur Implementierung von 2FA: https://atwork.safeonweb.be/de/MFA

- **Machen Sie Ihr Unternehmen konform mit dem ZCB Cyber Fundamentals Framework**

Das ZCB verfügt über ein Framework namens Cyber Fundamentals, das Organisationen zu einer angebrachten Cyber-Resilienz führt. Wir fordern alle Verwaltungen und öffentlichen Einrichtungen dazu auf, das entsprechende Niveau der Cyber Fundamentals als Sicherheitsstandard für ihre Organisation einzuführen. Das ZCB stellt auch ein einfaches Instrument zur Verfügung, mit dem sich das entsprechende Niveau leicht ermitteln lässt.
Weitere Informationen über das Cyber Fundamentals Framework: https://atwork.safeonweb.be/de/tools-resources/cyberfundamentals-framework

- **Verwaltungen und öffentliche Einrichtungen lassen sich nicht erpressen**

Das ZCB rät, dass Ransomware-Zahlungen kollektiv behandelt werden sollten, um das Ransomware-Geschäftsmodell zu untergraben und kriminelle Aktivitäten zu stören. Wir werden die erpresserischen Aktionen dieser Cyberkriminellen nicht tolerieren.
Daher raten wir dringend davon ab, eine Ransomware-Forderung zu bezahlen. Zahlung von Lösegeld an Ransomware-Akteure:

- garantiert nicht das Ende eines Vorfalls oder die Entfernung von Schadsoftware;
- ermutigt Kriminelle, ihre Aktivitäten fortzusetzen und auszuweiten;
- stellt kriminellen Akteuren zusätzliche Ressourcen zur Verfügung;
- garantiert nicht, dass Sie Ihre Daten wiederherstellen können oder dass sie nicht veröffentlicht werden.

Miguel De Bruycker
Generaldirektor ZCB