Safeonweb
@Work

EINE INITIATIVE VON

CENTRE FOR CYBER SECURITY BELGIUM

CYBER GRUNDLAGEN

SMALL

Version 2023-03-01

Zentrum für Cybersicherheit Belgien
18 Rue de la Loi
1000 Brüssel
Belgien

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

UNDER THE AUTHORITY
OF THE PRIME MINISTER

Inhaltsangabe

Einführung

Der **CCB Cyberfundamentals Framework** ist eine Reihe konkreter Maßnahmen, um:

- Daten zu schützen,
- das Risiko der häufigsten Cyberangriffe deutlich zu verringern,
- die Cyber-Resilienz einer Organisation zu erhöhen.

Um den Schweregrad der Bedrohung, welcher eine Organisation ausgesetzt ist, zu berücksichtigen, werden zusätzlich Ausgangsstufe ***Small*** drei weitere Sicherheitsstufen angeboten: ***Basic, Wichtig und Wesentlich***.

Die **Einstiegsstufe Small** ermöglicht einer Organisation eine erste Bewertung, wobei die Aspekte im Zusammenhang mit der internen Entwicklung von Anwendungen ausgeklammert werden.

Die Einstiegsstufe Small ist für Kleinstorganisationen (außer in einem Umfeld mit hohem Risiko) oder Organisationen mit begrenzten technischen Kenntnissen gedacht.

Der Framework ist ein lebendiges Dokument und wird unter Berücksichtigung des Feedbacks der Interessengruppen, des sich entwickelnden Risikos spezifischer Cybersicherheitsbedrohungen, der Verfügbarkeit technischer Lösungen und fortschreitender Erkenntnisse, ständig aktualisiert und verbessert.

1 ALLE ANMELDUNGEN MIT MULTI-FAKTOR-AUTHENTIFIZIERUNG SCHÜTZEN

Verwenden Sie die Multi-Faktor-Authentifizierung wann immer möglich. Verwenden Sie beim Fernzugriff immer die Multi-Faktor-Authentifizierung

Leitfaden

Die meisten Tools für die Multi-Faktor-Authentifizierung kombinieren Ihr Passwort mit Dingen, die Sie haben (Smartphone, Ausweis, ID-Karte) oder die Sie sind (Fingerabdruck). Die Verwendung mehrerer Elemente zur Authentifizierung verringert das Risiko eines Hackerangriffs.

- Verwenden Sie eine Passphrase, eine Zusammenstellung von mindestens drei zufälligen, gebräuchlichen Wörtern, die zu einer Phrase kombiniert werden und eine sehr gute Kombination aus Einprägsamkeit und Sicherheit bieten.Wenn Sie sich für ein typisches Passwort entscheiden:
  - Machen Sie es lang, mit Klein- und Großbuchstaben, eventuell auch Zahlen und Sonderzeichen.
  - Vermeiden Sie offensichtliche Wörter wie "Passwort", Buchstaben- oder Zahlenfolgen wie "abc" oder Zahlen wie "123".
  - Vermeiden Sie es, persönliche Informationen zu verwenden, die online zu finden sind.
- Und ob Sie Passphrasen oder Passwörter verwenden
  - Sie dürfen nicht anderweitig verwendet werden.
  - Ändern Sie Ihr Passwort, sobald der Verdacht besteht, dass es kompromittiert wurde.
- Aktivieren Sie die Multi-Faktor-Authentifizierung. Es gibt eine Vielzahl von MFA-Tools. Am besten wählen Sie ein MFA-Tool, das eine Vielzahl von Authentifizierungsoptionen bietet.
  MFA ist von größter Bedeutung für Systeme, die mit dem Internet verbunden sind, wie z. B. Fernzugriff. Der Fernzugriff kann z.B. über VPN (Virtual Private Network), RDP (Remote Desktop Protocol) realisiert werden.

2 INSTALLIEREN SIE SOFORT ALLE SICHERHEITSUPDATES

Implementieren Sie Sicherheitsupdates/Patches für Ihre gesamte Software, sobald sie verfügbar sind.

Leitfaden

- - Angesichts der Tatsache, dass Entwickler mit Cyberkriminellen darum kämpfen, ihre Software sicherer und weniger anfällig für die neuesten Angriffe zu machen, ist die schnellstmögliche Bereitstellung von Patches der Schlüssel zu mehr Cybersicherheit.Beachten Sie die folgenden Maßnahmen:
  - Beschränken Sie sich darauf, nur die Anwendungen (Betriebssysteme, Firmware oder Plugins) zu installieren, die Sie für den Betrieb Ihrer Organisation benötigen.
  - Installieren Sie nur vom Hersteller unterstützte Versionen der Software, die Sie verwenden möchten.
  - Automatisieren Sie den Aktualisierungsprozess so weit wie möglich, indem Sie automatische Updates als Standardeinstellung auf den Betriebssystemen Ihrer Endgeräte festlegen.
  - Es gibt Produkte, die Ihr System scannen und Sie benachrichtigen können, wenn es eine Aktualisierung für eine von Ihnen installierte Anwendung gibt. Wenn Sie eines dieser Produkte verwenden, stellen Sie sicher, dass es für jede von Ihnen verwendete Anwendung nach Updates sucht. Wenn Sie diese Produkte nicht verwenden, legen Sie einen Tag im Monat fest, an dem Sie die Verfügbarkeit neuer Patches prüfen und diese installieren.

3 ANTIVIRUS INSTALLIEREN

Implementieren Sie eine Antivirenlösung auf allen Gerätetypen und halten Sie sie auf dem neuesten Stand, um ihre ständige Wirksamkeit zu gewährleisten.

Leitfaden

Auch mit den besten Vorsichtsmaßnahmen können Sie mit dem Eindringen eines Virus oder einer Malware konfrontiert werden. Eine Anti-Malware-Software ist eine zweite Barriere, die Sie vor den Auswirkungen von Cyber-Vorfällen schützt.

- Die ausgewählte Anti-Malware-Software sollte vor allen Arten von Malware wie Viren, Spyware, Adware und Rootkits schützen.
- Es wird empfohlen, die Anti-Malware-Software so einzustellen, dass sie mindestens täglich (oder wenn verfügbar in "Echtzeit") automatisch nach Updates sucht und dann bald einen vollständigen Scan durchführt. Wenn mehrere Geräte (Heimcomputer, Laptops, Tablets...) verwendet werden, sollte die Anti-Malware-Software auf all diesen Geräten installiert und aktualisiert werden.
- Als Vorbeugungsmaßnahme sollten die folgenden Regeln angewendet werden:
  - Tauschen Sie keine USB-Laufwerke oder externen Festplatten zwischen privaten und geschäftlichen Computern oder Geräten aus.
  - Schließen Sie keine unbekannte / nicht vertrauenswürdige Hardware an Ihr System oder Netzwerk an und stecken Sie keine unbekannten externen USB-Laufwerke ein. Auf diesen Geräten kann sich Malware befinden. Deaktivieren Sie die AutoRun-Funktion für tragbare Laufwerke (USB, optische Laufwerke...) auf Ihren Geschäftscomputern, um zu verhindern, dass solche bösartigen Programme auf Ihren Systemen installiert werden.
  - Installieren Sie keine raubkopierte Software, da sie Malware enthalten kann.

4 SICHERN SIE IHR NETZWERK

Schützen Sie Ihr Netzwerk durch die Installation einer Firewall.

Schützen Sie die Daten im Netzwerk, auf die über WiFi zugegriffen wird, mit Hilfe von drahtlosen Verschlüsselungsstandards.

Achten Sie besonders auf die Sicherheit beim Fernzugriff.

Leitfaden

- Geben Sie Ihre WIFI-Passwörter nicht an andere weiter.
- Trennen Sie bei Bedarf Ihr WIFI-Netzwerk für Gäste/Besucher von Ihrem beruflichen Netzwerk.
- Zwischen Ihrem internen Netz und dem Internet sollten Firewalls installiert und konfiguriert werden. Dies kann eine Funktion eines (drahtlosen) Zugangspunkts/Routers sein, oder es kann eine Funktion eines Routers sein, der vom Internetdienstanbieter (ISP) bereitgestellt wird. Die Firewalls sollten aktiviert und aktualisiert werden. Sie können den Dienstleistungskatalog Ihres Internetanbieters auf die angebotenen Netzwerksicherheitsdienste überprüfen.
  - Stellen Sie sicher, dass das administrative Passwort Ihrer Firewall bei der Installation und danach regelmäßig geändert wird. Denken Sie auch daran, den Login des Administrators zu ändern
  - Die Verschlüsselung macht Ihre elektronisch gespeicherten Informationen für jeden unlesbar, der nicht das richtige Passwort oder den richtigen Schlüssel hat. Stellen Sie Ihren Router so ein, dass er mindestens WiFi Protected Access (WPA-2 oder WPA-3, wenn möglich) mit dem Advanced Encryption Standard (AES) zur Verschlüsselung verwendet.

5 SICHERN SIE IHRE DATEN

Führen Sie regelmäßig automatische Sicherungen Ihrer Daten durch.

Legen Sie wöchentlich oder alle paar Wochen eine Sicherungskopie OFFLINE(nicht an das Netz angeschlossen).

Sichern Sie Ihre Systeme nach größeren Änderungen, damit Sie sie leichter wiederherstellen können.

Leitfaden

Denken Sie daran, wie sehr Sie sich auf Ihre unternehmenskritischen Daten verlassen. Durch das Erstellen und Testen von Backups können Sie Ihre Daten und IKT-Systeme im Falle eines größeren Cybersicherheitsvorfall (z. B. eines Ransomware-Angriffs) wiederherstellen.
Einige grundlegende Leitlinien sind zu beachten:

- Ermitteln Sie, welche Daten Sie sichern müssen. Dies sind die wesentlichen Daten/Informationen, ohne die Ihr Unternehmen nicht funktionieren kann.
- Bestimmen Sie die Häufigkeit der Datensicherung auf der Grundlage der (aktualisierten oder erstellten) Datenmenge, die nach einem Ausfall verloren geht oder neu eingegeben werden muss.
- Trennen Sie die Sicherungsmedien von Ihren anderen Speichersystemen. Ein Offline-Backup ist sehr wichtig, um die Möglichkeit einzuschränken, dass Ihr Backup im Falle eines Hackerangriffs ebenfalls verschlüsselt oder vernichtet wird.
- Testen Sie die Wiederherstellung der Daten in regelmäßigen Abständen Es ist außerdem eine Basisprüfung, um festzustellen, ob das Backup-Verfahren einwandfrei funktioniert.

6 VERWALTUNGSRECHTE

Stellen Sie sicher, dass niemand mit Administratorrechten für tägliche Aufgaben arbeitet.

Leitfaden

Ein Administrator hat weitreichenden Zugang zu Ihrem System. Der Schutz dieser Konten ist sehr wichtig, da sie für Cyberkriminelle von großem Wert sind. Beachten Sie die folgenden Grundsätze zum Schutz dieser Konten:

- Trennen Sie Administratorkonten von Benutzerkonten. Für die tägliche Arbeit ist ein Benutzerkonto ohne Administratorrechte ausreichend.
- Verlangen Sie Multifaktor-Authentifizierung für alle Zugriffe auf Administratorkonten.

7 ABSCHLIESSENDE EMPFEHLUNGEN

Schützen Sie Ihre Computer und mobilen Geräte physisch vor Diebstahl oder unsachgemäßer Verwendung.

Beschränken Sie den Zugang zu Räumlichkeiten, Backups, Servern und Netzwerkkomponenten auf autorisierte Personen.

Wissen, wie und an wen man sich im Falle eines Cybervorfalls wenden kann.

Leitfaden

- Physische Sicherheit und Zugangsbeschränkung:
  - Physische Sicherheit ist der Schutz von Personal, Hardware, Software, Netzen und Daten vor physischen Einwirkungen und Ereignissen, die Ihrem Unternehmen ernsthafte Verluste oder Schäden zufügen könnten.
  - Es gibt erschwingliche Systeme für die Verwaltung mobiler Geräte, die eine Option sein können, wenn Sie viele mobile Geräte verwenden. Das Aktivieren von Anwendungen wie "Find My Phone" auf Ihren Mobiltelefonen kann ein erster Schritt sein.
  - Strenge Verwaltung der Schlüssel für den Zugang zu den Räumlichkeiten und der Alarmcodes.
- Im Falle eines Zwischenfalls:
  - Bewahren Sie eine Offline-Kopie (z. B. Offline-Festplatte oder -Laptop, Papierausdruck, ...) aller Dokumente auf, die Sie während eines Cybersicherheitsvorfalls oder einer Krise wahrscheinlich benötigen werden, indem Sie die folgenden Fragen beantworten:
    - An wen muss ich mich im Falle eines Cybervorfalls wenden?
    - Welche Informationen benötige ich, um sie zu kontaktieren?
    - Welche Informationen werden sie verlangen?
  - Für weitere Informationen stehen Ihnen unsere Empfehlungen im CCB-Leitfaden für das Management von Cybersicherheitsvorfällen zur Verfügung. Dieser bietet einen pragmatischen Ansatz für den Umgang mit Cybersicherheitsvorfällen und kann als Inspiration für Ihren eigenen Reaktionsplan oder Ihr Playbook dienen.

Haftungsausschluss

Dieses Dokument und seine Anhänge wurden vom Zentrum für Cybersicherheit Belgien (CCB) erstellt, einer föderalen Verwaltung, die durch den Königlichen Erlass vom 10. Oktober 2014 geschaffen wurde und dem Premierminister untersteht.

Dieses Dokument enthält technische Informationen, die hauptsächlich in Englisch verfasst sind. Diese Informationen über die Sicherheit von Netzen und Informationssystemen richten sich an IT-Dienste, die die englischen Begriffe der Computersprache verwenden. Eine Übersetzung dieser technischen Informationen ins Niederländische, Französische oder Deutsche kann jedoch bei der CCB angefordert werden.

Die CCB übernimmt **keine Verantwortung für den Inhalt** dieses Dokuments.
Die bereitgestellten Informationen:

- sind ausschließlich allgemeiner Natur und zielen nicht darauf ab, alle besonderen Situationen zu berücksichtigen.
- sind nicht notwendigerweise in allen Punkten erschöpfend, präzise oder auf dem neuesten Stand.

Verantwortlicher Redakteur

Zentrum für Cybersicherheit Belgien
Herr De Bruycker, Generaldirektor
Rue de la Loi, 18
1000 Brüssel

Juristisches Depot

D/2023/14828/001