Kontakt

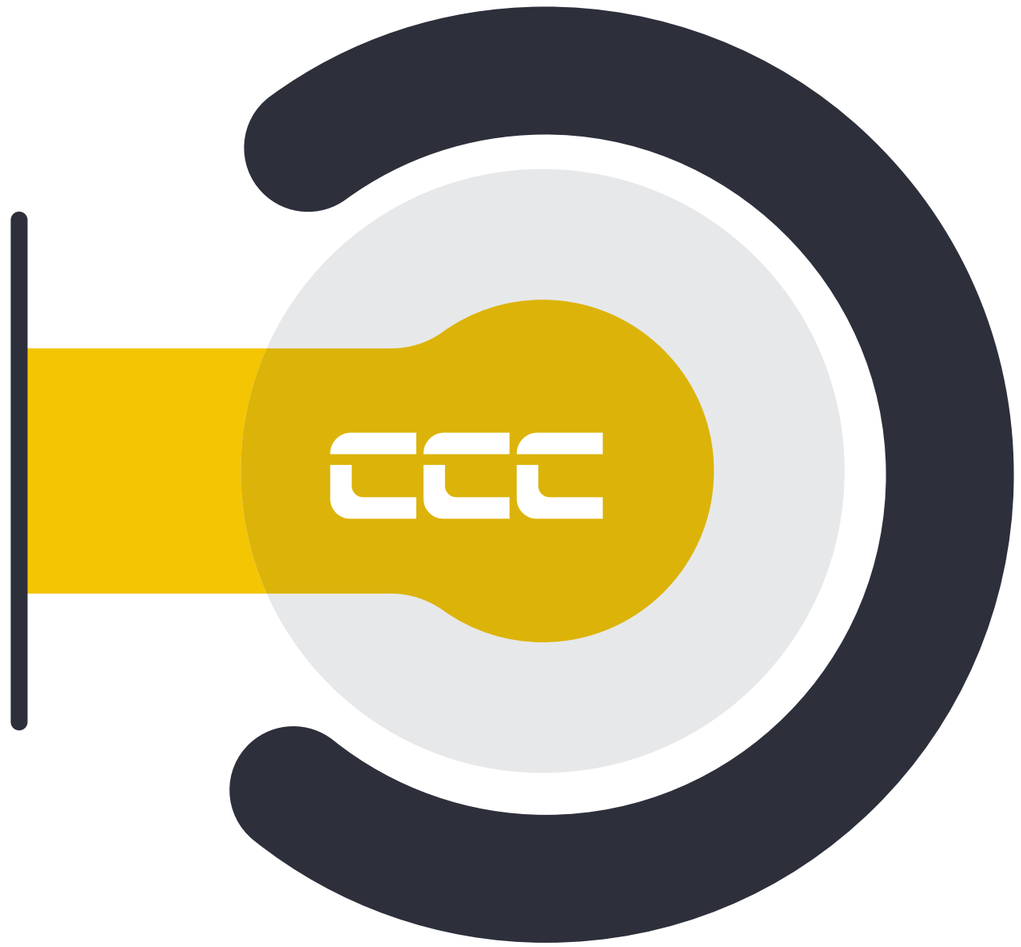
Weststraße 4
57392 Schmallenberg

P : 02972 96396-01

M : 0173 8253824

E : b.richter@cybercomplete.de

w : www.cybercomplete.de



CYBERSICHERHEIT **mit NIS2**

Unser
Unternehmen

Das Team der Cyber Complete GmbH versteht die Informationssicherheit als ganzheitlichen Ansatz und eine der wichtigsten Säulen in heutigen Unternehmen. In der Industrie- und Wirtschaftswelt des 21. Jahrhunderts ist inzwischen eine Vernetzung und Globalisierung gegeben, die eine Cybersicherheit für Unternehmen, Konzerne und Privatpersonen unabdingbar macht und eine Grundvoraussetzung für ein erfolgreiches Wirken ist. Täglich erfolgen aus allen Winkeln des Globus unzählige Hackerangriffe und Versuche, in die Systeme von Firmen einzudringen – die Tendenz ist weiter steigend. Auch politische Institutionen und ganze Regierungen sind von diesen Entwicklungen betroffen, besonders wenn es dabei um sensible und besonders schützenswerte Inhalte und Daten geht.

Inhaltsverzeichnis

Leitlinien & Richtlinien

Durch das Aufstellen von Leitlinien und Richtlinien werden intern Methoden angelegt, wie mit Daten umgegangen werden soll. Dieser Vorgang legt den Grundstein zur Wahrung von Informationssicherheit und dem Schutz der Privatsphäre.

Cyber Complete berät bei der Erstellung von Richtlinien und untersucht, ob Änderungen bei aktueller Richtlinien notwendig werden.

Prozessmanagement

Um die Effektivität von internen Maßnahmen zu prüfen ist es dringend empfohlen, Prüfmethoden und -zyklen festzulegen, die Sicherheitsmaßnahmen untersuchen.

Cyber Complete bietet Audits an, welche die Maßnahmen begutachtet und bewertet.

Business Continuity

Im Rahmen von Business Continuity Management (BCM) werden die potenziellen Bedrohungen ermittelt und vorbeugend Strategien, Prozesse sowie Maßnahmen entwickelt, mit denen die Geschäftsfähigkeit eines Betriebs oder einer Organisation im Ernstfall sichergestellt werden kann.

In einem mehrtätigen Audit wird der aktuelle Reifegrad ihrer Informationssicherheit ermittelt. Daraus leiten sich die Unternehmensziele in einem Maßnahmenplan ab.

Veeam
Contechnet
Freicon

- ✓ **Backupstrategie**
- ✓ **Krisenmanagement**
- ✓ **Wiederherstellung**
- ✓ **Penetration Testing**
- ✓ **ITIL-Prozesse**

Incident Management

Incident Management bzw. Incident Response Management beschreibt einen Prozess, bei dem Incidents erkannt und behoben werden, welche die IT-Services eines Unternehmens bedrohen oder stören.

In einem mehrtätigen Audit wird der aktuelle Reifegrad ihrer Informationssicherheit ermittelt. Daraus leiten sich die Unternehmensziele in einem Maßnahmenplan ab.

Notfallkommunikation
Krisenmanagement

Threat Intelligence
ForeNova
Fortinet

SOC - Anbieter
CSOC
Indevis

Identity & Access Management

IAM ist entscheidend, um sensible Daten und Ressorcen vor unbefugtem Zugriff zu schützen und gleichzeitig sicherzustellen, dass autorisierte Benutzer ihre Aufgaben effizient erledigen können.

Es spielt eine wichtige Rolle in modernen IT-Umgebungen, insbesondere mit dem Aufstieg von Remote-Arbeit und Cloud-Computing.

Authentifizierungs- und Autorisierungsmechanismen

.

Verschlüsselung

Die Verschlüsselung von Daten in den Stadien der Speicherung, Transport und Nutzung sichert, dass Diese nicht von Unbefugten abgegriffen werden können, wodurch die Vertraulichkeit von Informationen gewährleistet wird.

veeam
OpSwat

VPN (virtuelles privates Netzwerk)
ist ein Dienst, der den Internetverkehr in ungesicherten Netzwerken verschlüsselt und die IP-Adresse verbirgt, um die Online-Daten vor Dritten zu schützen.

- **Verschlüsselung Sicherungsmedien**
- **Schlüsselmanagement**

Schulungen

Der Faktor Mensch bleibt eine der größten Schwachstellen in der Cybersicherheit. Schulungen und Sensibilisierungsmaßnahmen werden wichtiger denn je sein, um Mitarbeiter vor sozialen Engineering-Angriffen zu schützen.

SoSafe
KnowBe4

- **lehren von Methoden, die Mitarbeiter und Betrieb vor Cyberattacken schützen**
- **Training Cyberhygiene**
- **Übungen zum Erkennen von Social Engineering-Attacken**

Cyber Complete gibt Mitarbeitern Werkzeuge und Wissen an die Hand, um den Betrieb vor Angriffen zu schützen.

Benjamin Richter, CEO

Einkauf
Life Cycle Management

Durch Wachsamkeit in Erwerb, Verwaltung, Wartung und Entsorgung am Ende des Betriebszeitraums von IT-Systemen wird das Risiko des Entstehens von Sicherheitslücken entgegen gewirkt.

- **Sicherheit beim Erwerb**
- **Wartungszyklen**
- **Patchmanagement**
- **Assetmanagement**

Baramundi

Sentinel One

Darknet Monitoring

Lieferkette
(Supply Chain)

Sicherheitsmaßnahmen, welche für die Interaktion mit Teilnehmenden in der Lieferkette Implementiert werden stellen sicher, dass Angreifer im Gefährdungsfall den Zugang von diesen Externen in das interne Netz des Betriebs nicht ausnutzen können.

- **Monitoring**
- **Schwachstellenmanagement**
- **Email Security**

Cyber Security ist nicht länger eine Option, sondern eine Notwendigkeit, um unsere digitale Zukunft zu schützen.

Blick
in die Zukunft

Die Zukunft der Cybersicherheit wird von einer Reihe von Trends und Entwicklungen geprägt sein, die auf die ständig wachsenden und sich verändernden Bedrohungen im digitalen Raum reagieren. Hier sind einige Schlüsselaspekte der zukünftigen Cybersicherheit.

Künstliche Intelligenz und maschinelles Lernen

Diese Technologien werden immer mehr in Sicherheitslösungen integriert, um Anomalien zu erkennen, Bedrohungen vorherzusagen und automatisierte Reaktionen auf Vorfälle zu ermöglichen.

IoT-Sicherheit

Mit der zunehmenden Verbreitung von Internet of Things (IoT)-Geräten werden Sicherheitslösungen notwendig, die diese Geräte absichern und sie vor Missbrauch schützen.

Zero-Trust-Modell

Dieses Modell geht davon aus, dass niemandem, weder innerhalb noch außerhalb des Netzwerks, uneingeschränktes Vertrauen geschenkt werden sollte. Jede Aktivität und jeder Zugriff wird permanent überprüft und validiert.

Cloud-Sicherheit

Da immer mehr Unternehmen auf Cloud-Dienste umsteigen, wird die Sicherheit dieser Dienste eine kritische Rolle spielen. Cloud-orientierte Sicherheitslösungen und -praktiken werden weiterentwickelt, um Daten und Anwendungen zu schützen.

Sicherheit für kritische Infrastrukturen

Die Sicherheit von kritischen Infrastrukturen wie Energieversorgung, Verkehrssystemen und Gesundheitswesen wird eine wachsende Priorität darstellen, da Angriffe auf diese Systeme erhebliche Auswirkungen auf die Gesellschaft haben könnten.

Menschliche Faktoren

Der Faktor Mensch bleibt eine der größten Schwachstellen in der Cybersicherheit. Schulungen und Sensibilisierungsmaßnahmen werden wichtiger denn je sein, um Mitarbeiter vor sozialen Engineering-Angriffen zu schützen.

> ***Die Zukunft der Cybersicherheit wird von einer Mischung aus fortschrittlichen Technologien, neuen Sicherheitsansätzen und erhöhtem Bewusstsein für die Bedeutung der Sicherheit im digitalen Zeitalter geprägt sein.***