Kontakt

Weststraße 4
57392 Schmallenberg

P : 02972 96396-01

M : 0173 8253824

E : b.richter@cybercomplete.de

w : www.cybercomplete.de

CYBER COMPLETE CORPORATION

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 Privat-personen 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.

Fachbereiche

Unsere
Geschäftsführung

Benjamin Richter und sein Team sind bereits über 20 Jahre in der IT-Welt zu Hause.

Ihre Erfahrung konnten sie in unzähligen Projekten zur IT-Sicherheit, Finance und ERP sammeln.

Unser
Team

“Wir arbeiten als Team und sind in unseren Bereichen ausgewiesene Experten.”

Benjamin Richter
Senior Cyber Architect

Sebastian Rinne
Vertriebsleiter

Georg Schneider
IT-Leiter

Jacqueline Webb
IT-Support

Unsere Leistungen

Analyse und Dokumentation des IST-Zustandes.

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

Regelmäßige Security-Audits

Bei Durchführung von regelmäßigen IT Sicherheits-Audits im Unternehmen wird sichergestellt, dass die implementierten Schutzmaßnahmen effektiv sind und greifen.

Information Security Management System

Durch unsere Erfahrung beraten und begleiten wir Kunden zur erfolgreichen Einführung eines ISMS. Dies kann eine ISO 27001, TISAX, DORA oder NIS 2 sein.

Durchführung Awareness Kampagnen

Häufig sind es Mitarbeiter, welche durch Unwissen zum Teil großen Schaden in Unternehmen anrichten können. Somit sind regelmäßige Schulungen unersetzbar.

Die Verteidigung der digitalen Welt

Die Bedrohungslandschaft in der Cyberwelt ist ständig im Wandel. Hacker und Angreifer entwickeln immer raffiniertere Techniken, um Schwachstellen in digitalen Systemen auszunutzen. Einige der aktuellen Bedrohungen umfassen:

- **Malware:** Schädliche Software wie Viren, Trojaner und Ransomware kann dazu verwendet werden, Daten zu stehlen, Systeme zu blockieren oder sogar Geld von Opfern zu erpressen.
- **Phishing:** Diese Technik zielt darauf ab, Benutzer zur Preisgabe persönlicher Informationen wie Passwörter oder Kreditkartendaten zu verleiten, indem sie vorgeben, von vertrauenswürdigen Quellen zu stammen.
- **DDoS-Angriffe:** Distributed Denial of Service-Angriffe überfluten Websites oder Online-Dienste mit Traffic, um sie zu überlasten und unzugänglich zu machen.
- **Zero-Day-Exploits:** Das sind Schwachstellen in Software oder Hardware, die noch nicht bekannt sind und von Angreifern ausgenutzt werden, bevor die Hersteller Abhilfemaßnahmen entwickeln können.

Unternehmenswerte schützen

- **Cyber Security ist Chefsache**
- **Abstimmung gemeinsamer IT-Strategien**
- **Aufbau und Doku von Rollen & Prozessen**
- **Härtung der technischen IT-Komponenten**
- **Notfallmanagement und Krisenplanung**
- **Awareness-Kampagnen für Mitarbeiter**

ISMS Projektpartner

“Damit wir als Cyber-Architekten alle notwendigen Bereiche in den Unternehmen abdecken können, haben wir starke Partner zur Unterstützung an unserer Seite!”

SentinelOne 01

SentinelOne schützt Endpoints, Cloud, Identitäten sowie Daten und reduziert dabei die Komplexität, Risiken und Kosten mithilfe von KI und gezielter Automatisierung. Hierbei unterstützen Dashboards in einem 24/7 Managed Services und aktives Threat Hunting.

SonicWall 02

SonicWall bietet Sicherheitslösungen im Netzwerk an. Du den Produkten gehören Firewalls, VPNs, sichere E-Mail-Gateways und Endpoint Protection. Die Lösungen sind allesamt darauf ausgelegt, Daten, Netzwerke und Geräte vor Cyberbedrohungen ganzheitlich zu schützen.

KnowBe4 03

Das automatisierte Security Awareness Programm von KnowBe4 erleichtert Ihnen Ihre Arbeit rund um die Themen Compliance. Mit konkreten Empfehlungen, wertvollen Tipps, hilft KnowBe4 Ihnen dabei, Gefahren durch Social Engineering, Phishing und Ransomware-Angriffen mithilfe von speziellen Trainings zu bewältigen.

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

Zufriedene Kunden

"In unserem Projekt zum Information Security-Management-System konnten Benjamin Richter und sein Team ihre Expertise erfolgreich unter Beweis stellen."

- Geschäftsführer Sebastian Pöppel -

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.