Leitfaden für Cybersicherheit

für die Entscheidungsträger und

Führungskräfte

Kontaktieren Sie uns jetzt und
erhalten Sie eine kostenlose Demo!

Die 10 häufigsten Cyberbedrohungen

Fortgeschrittene anhaltende Bedrohungen (APTs): APTs sind gezielte und ausgeklügelte Angriffe, die oft mit Nationalstaaten oder organisierten cyberkriminellen Gruppen in Verbindung gebracht werden. Die Kriminellen zielen darauf ab, für längere Zeit unentdeckt zu bleiben und sensible Daten zu stehlen.

Datenschutzverletzungen: Bei Datenschutzverletzungen handelt es sich um den unbefugten Zugriff auf sensible Daten, der zu Datendiebstahl, finanziellen Verlusten und Rufschädigung führen kann.

Social Engineering: Bei Social-Engineering-Angriffen werden Personen dazu gebracht, vertrauliche Informationen preiszugeben. Sie können verschiedene Formen annehmen, z. B. Pretexting, Lockangebote oder Tailgating.

Ransomware: Ransomware verschlüsselt die Daten eines Unternehmens und verlangt für die Entschlüsselung ein Lösegeld. Sie kann den Betrieb stören und zu finanziellen Verlusten führen.

Zero-Day-Schwachstellen: Hierbei handelt es sich um Software-Schwachstellen, die dem Hersteller unbekannt sind und von Angreifern ausgenutzt werden. Zero-Day-Angriffe können sehr schädlich sein.

Malware (z. B. Viren, Ransomware, Trojaner): Malware ist bösartige Software, die darauf abzielt, Computersysteme zu infiltrieren oder zu beschädigen. Sie kann zu Datenschutzverletzungen, finanziellen Verlusten und Systemunterbrechungen führen.

Phishing-Angriffe: Phishing ist eine Taktik, bei der Cyberkriminelle mit Hilfe von betrügerischen E-Mails oder Nachrichten Personen dazu bringen, sensible Informationen wie Anmeldeinformationen oder Finanzdaten preiszugeben.

IoT-Schwachstellen: Da immer mehr Geräte miteinander verbunden werden, können Schwachstellen in Internet-of-Things-Geräten (IoT) ausgenutzt werden, um unbefugten Zugang zu Netzwerken zu erhalten.

Distributed Denial of Service (DDoS)-Angriffe: DDoS-Angriffe überlasten die Onlinedienste oder die Website eines Unternehmens, verursachen Störungen und führen möglicherweise zu Ausfallzeiten und finanziellen Verlusten.

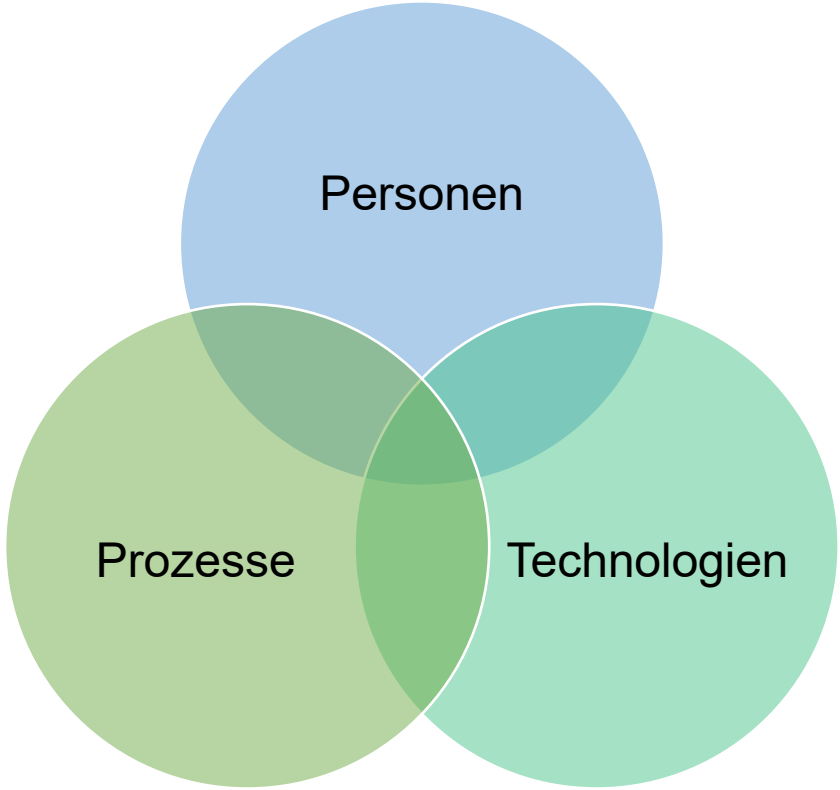
Insider-Bedrohungen: Insider-Bedrohungen gehen von aktuellen oder ehemaligen Mitarbeitenden, Auftragnehmern oder Partnern aus, die ihre Zugriffsrechte missbrauchen, um Daten zu stehlen oder dem Unternehmen zu schaden.

Kontaktieren Sie uns jetzt und erhalten Sie eine kostenlose Demo!

SPIE

Die 3 Hauptverteidiger

Der **SPIE-ICS-Ansatz** «Personen, Prozesse, Technologien» berücksichtigt, dass Cybersicherheit nicht nur eine technologische Herausforderung ist, sondern eine **ganzheitliche Aufgabe**, bei der Menschen, gut definierte Prozesse und geeignete Technologien zusammenarbeiten. Um sich wirksam vor Cyber-Bedrohungen zu schützen, **müssen Unternehmen alle drei Komponenten kontinuierlich berücksichtigen** und sich an die sich verändernde Bedrohungslandschaft anpassen.



Kontaktieren Sie uns jetzt und erhalten Sie eine kostenlose Demo!

SPIE ICS: Ihr Cybersicherheits-One-Stop-Shop

IMPLEMENTATION

Project Management

Installation, Configuration

Migration

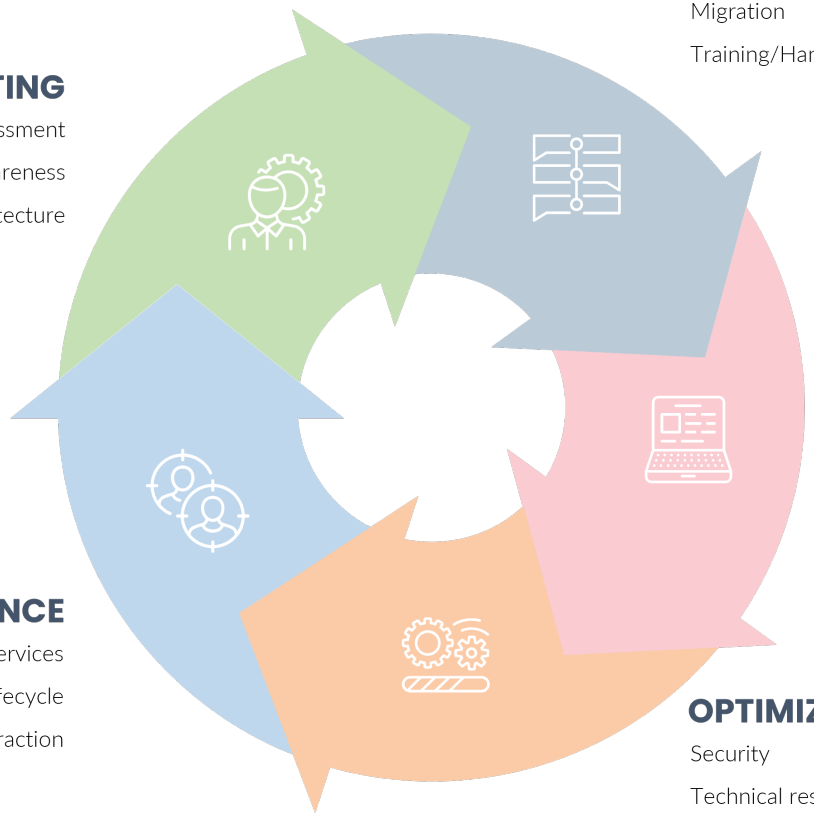
Training/Handover

CONSULTING

Cybersecurity Assessment

User Awareness

Security Strategy & Architecture



OPERATION

Managed Service

Incident Management

Proactive/reactive maintenance

Training/Handover

CUSTOMER EXPERIENCE

Adoption services

HW/SW lifecycle

Value extraction

OPTIMIZATION

Security

Technical resources

Sustainability

Kontaktieren Sie uns jetzt und
erhalten Sie eine kostenlose Demo!

Ihre 8 Vorteile

Kosteneinsparungen: Investitionen in Cybersicherheitsmassnahmen sind zwar mit Kosten verbunden, aber ein ganzheitlicher Ansatz hilft, diese Investitionen zu optimieren. Langfristig werden Sie Ihre Ressourcen effektiver einsetzen und Geld sparen.

Vereinfachtes Management: Die Zusammenarbeit mit SPIE ICS als Ihrem einzigen Dienstleister vereinfacht die Verwaltung Ihrer Cybersicherheitsinfrastruktur. Sie haben einen einzigen Ansprechpartner für alle Ihre Cybersicherheitsanforderungen, was die Kommunikation und Fehlerbehebung vereinfacht.

Schutz des Rufs: Eine Sicherheitsverletzung schadet Ihrem Ruf und untergräbt das Vertrauen Ihrer Kundinnen und Kunden. Führungskräfte, die einen ganzheitlichen Ansatz für die Cybersicherheit verfolgen, sind besser darauf vorbereitet, Vorfälle zu verhindern und schnell zu reagieren, wenn diese eintreten. So minimieren sie den Imageschaden.

Langfristige Widerstandsfähigkeit: Unsere ganzheitliche Cybersicherheitsstrategie konzentriert sich auf die langfristige Widerstandsfähigkeit und nicht auf kurzfristige Problemlösungen. Sie treffen fundierte Entscheidungen, die die Fähigkeit Ihres Unternehmens stärken, den sich entwickelnden Cyber-Bedrohungen zu widerstehen.

Wettbewerbsvorteil: Unternehmen, die der Cybersicherheit mit SPIE ICS Priorität einräumen, nutzen ihr Engagement für Sicherheit als Wettbewerbsvorteil. Kunden und Kundinnen sowie Partner entscheiden sich für Unternehmen, die ein starkes Engagement für den Schutz von Daten und Privatsphäre zeigen.

Unterstützung von Innovationen: Eine starke Cybersicherheitsgrundlage, die von SPIE ICS unterstützt wird, ermöglicht sichere Innovationen und digitale Transformationsbemühungen. Sie können selbstbewusst neue Technologien und Geschäftsmodelle erforschen und gleichzeitig die Sicherheit aufrechterhalten.

Vertrauen des Vorstands und der Stakeholder: Führungskräfte, die mit SPIE ICS einen ganzheitlichen Cybersicherheitsansatz verfolgen, schaffen Vertrauen beim Vorstand, bei Investorinnen und Investoren und bei anderen Interessengruppen. Dies wirkt sich positiv auf die Gesamtführung des Unternehmens aus.

Sicherheit der Lieferkette: Ein ganzheitlicher Ansatz erstreckt sich auch auf Drittanbieter und Partner. SPIE ICS stellt sicher, dass Ihre Lieferkette die Sicherheitsstandards einhält und minimiert Schwachstellen, die von externen Verbindungen herrühren.

Kontaktieren Sie uns jetzt und
erhalten Sie eine kostenlose Demo!