ÜBER EXPERTCIRCLE

Die ExpertCircle GmbH hat sich das Ziel gesetzt, basierend auf dem Wissen der qualifizierten Mitarbeiter und deren langjährigen Erfahrungen im IT-Dienstleistungsumfeld die bestmögliche IT-Plattform für ihre Kunden zu realisieren. Schwerpunkte bilden hierbei die Themenbereiche Systems Management, Security Management und Core Infrastructure. Durch die Nähe zu ihren Kunden ist die ExpertCircle GmbH in der Lage, deren Business und die damit verbundenen Anforderungen an die Informationstechnologie zu verstehen, um geeignete Lösungen auf Basis am Markt etablierter Standards anzubieten.

Die Critical Security Controls und deren Weiterentwicklung werden vom Council on CyberSecurity verwaltet.

www.counciloncybersecurity.org/critical-controls
www.sans.org/critical-security-controls

und unter Creative Commons 3.0 lizenziert: http://creativecommons.org/licenses/by-nd/3.0/

ExpertCircle GmbH

Verwaltungssitz:
Nordstraße 9
56424 Mogendorf

Niederlassung:
Mittelstraße 2-10
53173 Bonn

Fon: +49 2623 929851-0
Fax: +49 2623 929851-19

www.expertcircle.de
info@expertcircle.de

Wissen. Erfahrung. Nähe.
EXPERTCIRCLE

EXPERTCIRCLE

Ressourcen bestmöglich nutzen. Risiken praktikabel reduzieren.

WORKSHOP INFOSEC AWARENESS

CRITICAL SECURITY CONTROLS FOR EFFECTIVE CYBER DEFENSE

RISIKEN FÜR JEDE IT-STRUKTUR PRAKTIKABEL REDUZIEREN

www.counciloncybersecurity.org/critical-controls
www.sans.org/critical-security-controls

Inventar autorisierter und nicht autorisierter Geräte	Nur autorisierte Geräte dürfen Zugriff zum Netzwerk erhalten. Nicht autorisierte und nicht gemanagte Geräte werden erkannt, ihr Zugriff wird unterbunden.
Inventar autorisierter und nicht autorisierter Software	Nur autorisierte Software darf im Netz installiert und ausgeführt werden. Nicht autorisierte und nicht verwaltete Software wird erkannt, ihre Installation und Ausführung wird unterbunden.
Sichere Konfiguration für Hardware & Software auf Laptops, Workstations und Servern	Konfigurations- und Change-Management-Verfahren für Sicherheitseinstellungen auf Laptops, Servern und Workstations, um Angriffsmöglichkeiten zu reduzieren.
Kontinuierliche Schwachstellenanalyse und -vorsorge	Kontinuierliches Prüfen auf Sicherheitslücken und Beseitigen bekannter Schwachstellen, um das Zeitfenster für potenzielle Angriffe zu minimieren.
Schutz vor Malware	Überwachen von Verbreitung und Ausführung von Schadcode. Optimieren automatischer Abwehr- und Korrekturmaßnahmen.
Sicherheit in Applikationssoftware	LifeCycle Management sämtlicher selbst entwickelter und erworbener Software, um Sicherheitslücken zu verhindern, zu entdecken und zu korrigieren.
Kontrolle der WLAN Infrastruktur	Sichere Konfiguration und sicherer Betrieb kabelloser Netze und derer Komponenten.
Datenwiederherstellungskapazitäten (Backup & Restore)	Prozesse und Technologien implementieren, um kritische Daten in definierten Zeitrahmen und zu einem definierten Stand wiederherstellen zu können (RTO/RPO).
Sicherheitsqualifikation und Sicherheitstrainings	Alle unternehmenskritischen Funktionsrollen benötigen ausreichende Kenntnisse, um das Unternehmen vor Schäden zu schützen. Wissenslücken müssen identifiziert und durch Schulungen und Awareness-Maßnahmen behoben werden.
Sichere Konfiguration von Netzwerk Geräten	Konfigurations- und Change-Management-Verfahren für Sicherheitseinstellungen auf Netzwerksystemen wie Firewalls, Router, Switchen etc., um Angriffsmöglichkeiten zu reduzieren.

ExpertCircle

Einschränkung und Kontrolle von Netzwerk-Ports	Reduzierung und Management operativ verwendeter Netzwerk-Ports, -Protokolle und -Dienste minimieren das Risiko potenzieller Angriffe.
Kontrollierter Einsatz administrativer Privilegien	Prozesse und Instrumente zur Vergabe und Kontrolle administrativer Rechte auf Systemen und in Anwendungen.
Perimeterschutz	Kontrolle des Netzwerkverkehrs zwischen Netzwerksegmenten mit unterschiedlichen Sicherheitsniveaus (Intranet-DMZ-Extranet-Internet).
Pflege, Monitoring und Analyse von Sicherheits- und Audit Logs	Sammeln, Verwalten und Auswerten von Überwachungsprotokollen und Sicherheitslogs, um Angriffe zu erkennen und zu verstehen oder erfolgreiche Angriffe zu analysieren.
Zugriffskontrolle auf Basis „Need to Know“	Prozesse und Instrumente zur Vergabe und Kontrolle geregelter Zugriffe auf unternehmenskritische Daten, Ressourcen und Systeme.
Kontenverwaltung und -überwachung	LifeCycle Management und Überwachung von System- und Anwendungskonten.
Datenschutz und DLP	Prozesse und Instrumente zum Gewährleisten der Vertraulichkeit und Unversehrtheit sensibler Daten und zum Verhindern von Datendiebstahl und unbeabsichtigtem Datenverlust.
Incident Response und Incident Management	Entwicklung und Umsetzung einer Incident-Response-Infrastruktur (Prozesse, Rollen, Pläne, Training, etc.), um Sicherheitsvorfälle schnell zu erkennen, Angriffe abzuwehren und potenziellen Schaden zu minimieren.
Sicheres Netzwerkdesign	Designvorgaben und Sicherheitsfunktionen, die eine zuverlässige IT-Infrastruktur gewährleisten und potenzielle Angriffsvektoren minimieren (Defense in Depth).
Penetrationstests und Angriffsübungen (Red Team Exercises)	Simulation realer Angriffe, um das aktuelle Sicherheitsniveau sowie getroffene Sicherheitsmaßnahmen zu prüfen.

ExpertCircle

RESSOURCEN BESTMÖGLICH NUTZEN.

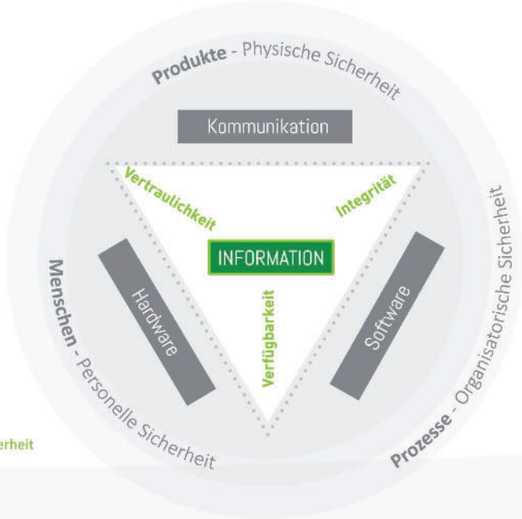
WORKSHOP INFOSEC AWARENESS

DAS NOTWENDIGE MÖGLICH MACHEN

Wachsende Anforderungen an zunehmend komplexe IT-Infrastrukturen, aber auch Cloud Computing und wachsender Datentransfer über Unternehmensgrenzen hinweg stellen IT-Verantwortliche vor die große Herausforderung, Ressourcen für IT-Sicherheit optimal einzusetzen, um den bestmöglichen Nutzen mit ihnen zu erzielen. Dabei gilt es, die Balance zwischen Sicherheit und Verfügbarkeit sowie Bedienbarkeit und Kostenreduzierung zu finden.

Die Interpretation gesetzlicher Regelungen und anderer Compliance-Auflagen erschweren dies oft. Vielfach führen fehlende Vorgaben und Unsicherheit beim Einschätzen realer Risiken und derer möglichen Auswirkungen dazu, dass vorhandene Ressourcen nicht effizient eingesetzt werden und sinnvolle Sicherheitsmaßnahmen nicht ihre volle Wirkung entfalten.

Die ExpertCircle GmbH zeigt Unternehmen unter Verwendung des Frameworks der Critical Security Controls for Effectice Cyber Defense (siehe Inlay) praktikable Vorgehensweisen dafür auf, IT-Sicherheitsrisiken effektiv zu reduzieren. Dies bietet auch die Grundlage dafür, gesetzliche, unternehmensinterne und vertragliche Regelungen im IT-Umfeld einzuhalten.



Das Konzept der Information Security / Informationssicherheit

UNSER ANGEBOT

Workshop InfoSec

Eintägig bei Ihnen im Unternehmen, mit allen relevanten Ansprechpartnern.

Komplettpreis

2.800,00 €*

Jetzt ganz einfach buchen!

Telefon: +49 2623 929851-0
E-Mail: sales@expertcircle.de

DER WORKSHOP: WAS WIR TUN

Gemeinsam mit Ihnen und Ihren relevanten Fachkräften besprechen wir Ihre IT-Konzepte, Ihre Systemumgebung sowie aktuelle oder absehbare technische Anforderungen – dies jeweils im Kontext Ihrer geschäftlichen Anforderungen sowie potenzieller gesetzlicher oder anderer Compliance-Vorgaben. Wir identifizieren zusammen mögliche Risikobereiche zur Fokussierung der Ressourcen für die IT-Sicherheit auf die relevanten Bereiche. Hierbei sollen Risikobereiche klassifiziert und mögliche Auswirkungen auf Ihr Unternehmen abgeschätzt werden. Auf diese Weise wird es möglich, zwischen realen und eher abstrakten Risiken zu unterscheiden.

Im Vorgehen orientieren wir uns an den Critical Security Controls for Effective Cyber Defense als Framework für eine praktikable Risikoreduzierung. Soweit möglich, betrachten wir dabei Ihre Betriebsprozesse sowie betriebliche und operative Aspekte. Zu Beginn des Workshops stellen wir Ihnen das Framework der Critical Security Controls kurz vor.

... UND WAS SIE DARAUS MITNEHMEN:

- Ein zusammenfassendes Ergebnispapier
- Erste Bewertung identifizierter Risikobereiche inklusive für Ihr Business relevanter Impact
- Erste Handlungsempfehlungen mit Optimierungsmaßnahmen und Quick Wins
- Weitere Handlungsempfehlungen, wie zum Beispiel
  - tiefere Analyse definierter Bereiche
  - Vorschläge zu Architekturänderungen
  - Proof of Concept zusätzlicher Handlunsgmöglichkeiten

*(zzgl. MwSt + entfernungsabhängiger Nebenkosten)