An wen wendet sich CPS©041

- IT-Verantwortliche
- Informationssicherheitsbeauftragte
- IT-Administratoren
- Geschäftsführungen
- Externe Datenschutzbeauftragte
- Versicherungen
- u.s.w.

Wir empfehlen:

eLearning

Aufbau eines Datenschutz-Management-Systems gemäß

CPS©100
Konformitäts-Bewertungsprogramm

Haftungsmanagement Datenschutz, Informationssicherheit

Weitere CPS© verfügbar

In Zusammenarbeit mit IITR Datenschutz GmbH

IITR DATENSCHUTZ. RECHT. EINFACH.

Über IITR Cert GmbH

Auditierungen sowie Zertifizierungen werden durchgeführt auf Grundlage von:

privASSIST

Ein webbasiertes Instrument zur Fern-Auditierung u.a. von datenschutzrelevanten Vorgängen zur Auditierung und Dokumentation der IT-Sicherheit sowie dem Status von datenschutzrechtlichen Vorgaben.

CPS© Certified Privacy Standard (CPS)

Als Grundlage für Auditierungen und Zertifizierungen stehen Konformitätsbewertungs-Programme zur Verfügung.

Ralf Zlamal
Externer Datenschutzbeauftragter
Informationssicherheitsbeauftragter

+49 (0)89 1891 7360
email@iitr.de

IITR Cert GmbH · Marienplatz 2 · 80331 München
Geschäftsführer: Dr. Sebastian Kraska, Ralf Zlamal
Sitz: Eschenrieder Str. 62c, 82194 Gröbenzell
Amtsgericht München, HRB 188513

www.iitr-cert.de

privASSIST

IITR DATENSCHUTZ. RECHT. EINFACH.

Auditierung CPS©041 Cyber-Security

www.iitr.de

Cyber-Attacken und Cyber-Security

Einen verläßlichen Schutz gegen diese Art von Angriffen gibt es derzeit nicht. Dennoch sind Überlegungen angebracht, sich mit dieser Gefahr auseinanderzusetzen.

Die Kriminellen – häufig staatlich unterstützt – suchen sich den einfachsten Weg.

1. Darin liegt eine Chance, einem Angriff entgehen zu können

Wer schlecht aufgestellt ist, hat das höhere Risiko!

2. Backup Strategie
3. Ausreichendes IT-Budget, Investition in Know-how der Mitarbeiter
4. „Multi-Faktor-Authentifizierung"
5. Etablierung eines Systems zur Früherkennung

Angreifer sind in der Regel 2 - 3 Monate im Unternehmen bevor der Angriff offengelegt wird

Etablieren Sie einen Verantwortlichen, der die Früherkennung regelmäßig zu überwachen hat

Ohne Früherkennung sind Backups häufig keine Rettung, da Angriffe sich auf Backups erstrecken

6. Führen Sie Notfall-Tests durch

Wie verläßlich ist Ihr Backup-System?

CPS©041

Cyber-Security

Inhaltsangabe

CPS©041 beinhaltet **95 Fragen** zur Umsetzung Ihrer Cyber-Security mit folgenden Schwerpunkten:

1. IT-Allgemein
2. IT-Administration
3. Netzwerk
4. Zugangsschutz
5. Patch-Management
6. Backup & Wiederanlauf
7. WLAN
8. Penetrationstest
9. Schulung
10. Incident-Management
11. Schutz vor Schadsoftware etc.
12. Monitoring

Der Status-Report richtet sich an die für die IT-Sicherheit bzw. Cyber-Security verantwortliche Person innerhalb eines Unternehmens und sollte von dieser Person bearbeitet werden.

Ein Angriff hat stattgefunden

Zunächst muß ein Unternehmen seine Handlungsfähigkeit sicherstellen. Idealerweise wurde im Vorfeld eines möglichen Eintretens abnormaler Situationen ein Krisenteam zusammengestellt.

Seien Sie auf die Forderungen der Angreifer vorbereitet!

- Versuchen Sie nicht die Gegenseite zu überzeugen, dass sie etwas Kriminelles getan haben!
- Steigen Sie sofort in die Verhandlung ein! Die Zeit läuft gegen das Unternehmen!
- Lassen Sie sich einen Beweis vorlegen! Beispielsweise ob ein verschlüsseltes Dokument tatsächlich entschlüsselt werden kann.

Die Angreifer kennen Ihr Unternehmen und dessen finanzielle Leistungsfähigkeit. Verhandlungsteams der Angreifer bezeichnen die geforderten Summen i.d.R. nicht als verhandelbar.

Kriminelle sind derzeit im Vorteil!

Wir empfehlen auf einen Angriff vorbereitet zu sein.

Die Bereitstellung von Erpressungsgeld muß organisiert werden. Dieser Vorgang könnte längere Zeit in Anspruch nehmen, während Ihr Betrieb einen Ausfall hat!

Einen ersten Überblick über den Status und die damit möglichen Defizite Ihres Unternehmens verschafft Ihnen:

CPS©041 Cyber-Security

Unser Angebot für Ihr Unternehmen mittels einer durch privASSIST durchgeführten, webbasierten Auditierung.