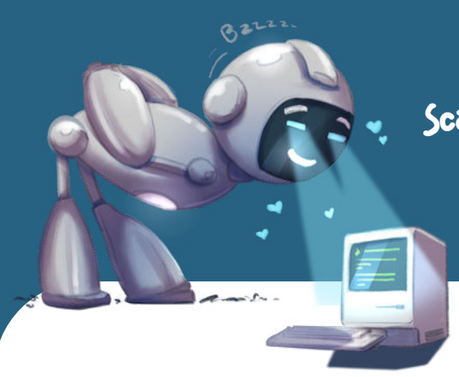
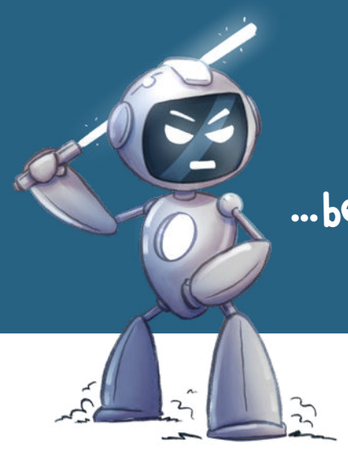
Cyberattacke Notfallplan



Scannt das Netzwerk...

...analysiert und berichtet...



...bekämpft die Bösen.

Notfall-Kontakte für Cyberangriff

Name/Person	Rolle oder Dienst	Zeitfrist	Team	Firma	Kontakt
.....	Informationssicherheits-beauftragter (ISB), CISO	15 min	IST	.....	.....
.....	IT-Leiter	15 min	IST	.....	.....
.....	Geschäftsführer/Vorstand	15 min	IST	.....	.....
Task Force Digitale Spuren	Strafverfolgungsbehörden, Cybercrime (Meldung nach IST Beschluss)	24 h		Polizei BaWü	0711 5401-2444 cybercrime@polizei.bwl.de
.....	Incident Response Service (Meldung nach IST Beschluss)	12 h		.....	.....
.....	Cyberversicherung Versicherungsnr.:			.....	.....

Merkmale eines Angriffs:

Beobachtung von **ungewöhnlichem Soft- u. Hardware-Verhalten & Verdacht** auf **Malware, Ransomware, Phishing** nach Ihrer Einschätzung gem. den Inhalten des Security Awareness Trainings!

Sofortmaßnahmen:

1) Die **Ruhe** bewahren, **Informationen** über Geräte/Software u. Symptome kurz sammeln!
2) Netzwerk trennen, PC **nicht** ausschalten!
3) Den **ISB, CISO** oder I**T-Leiter** umgehend direkt **kontaktieren** oder bei Abwesenheit per Telefon:
   Wer meldet? – Welches System ist betroffen? – Was ist zu beobachten? – Wann ist das Ereignis eingetreten? –
   Wo befindet sich das betroffene IT-System?
4) Den Anweisungen der **Notfallpläne** folgen - insbesondere der Meldekette!
   Die Notfallpläne liegen hier: .....
5) Den **Schaden einschätzen**: Protokollierung und Bewertung, eventuell mit dem IRS für forensische Untersuchungen
6) Die **Ersatzsysteme u. Prozesse** gem. ISMS (BCM) aktivieren!
   Das ISMS liegt hier: .....

Notfall-Kontakte für Datenschutzverletzung

Name	Rolle	Zeitfrist	Team	Firma	Kontakt
.....	Datenschutzmanager (DSM)	15 min	DST	.....	.....
.....	Datenschutzbeauftragter (DSB)	8 h	DST	.....	.....

Merkmale einer Datenschutzverletzung:

Personenbezogene Daten dürfen nach DSGVO nur gem. einer gewissen Zweckbestimmung und nur nach Freigabe durch die betroffene Person verarbeitet werden. Wenn Daten einer gewissen Datenschutzkategorie intern oder extern einer anderen Person **bekannt** werden, handelt es sich um eine Datenschutzverletzung.

Sofortmaßnahmen:

Versuchen Sie zuerst, den DSM persönlich zu kontaktieren. Sollte dies nicht erfolgreich sein, senden Sie eine E-Mail an den DSM.

Dieser Notfallplan orientiert sich an dem BSI-IT Grundschutz, ISO 27000 und VdS 10000.
Legende: ISB: Informationssicherheitsbeauftragter, DSM: Datenschutzmanager, DSB: Datenschutzbeauftragter, IST: Informationssicherheitsteam, DST: Datenschutzsicherheitsteam