snapSEC

Ihr Partner, wenn es um
IT-Sicherheit und Datenschutz geht

snapSEC

Incident Response Plan

- Vorbereitung
  - Richtlinien
  - Response Plan / Strategie
  - Kommunikation
  - Dokumentation
  - Team (CERT, CSIRT)
  - Zugriffskontrolle
  - Training
  - Tools

snapSEC

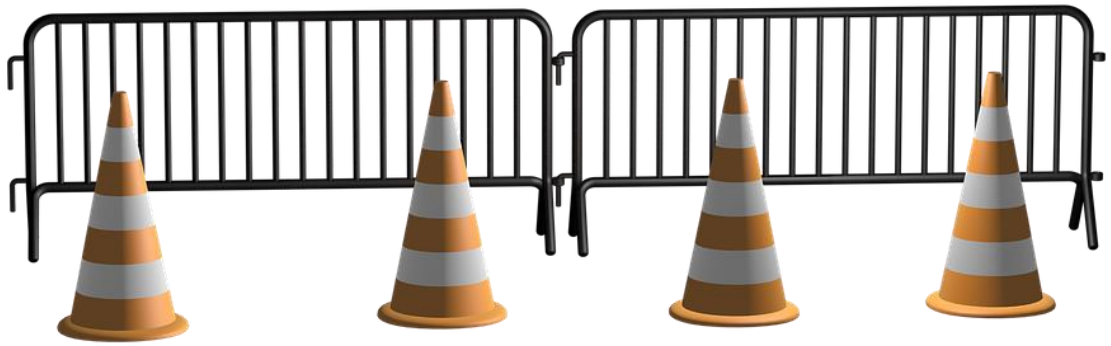
Incident Response Plan

- Identifikation
  - Security-Monitoring
  - Event-Management/-Analyse
  - Incident-Identifizierung
  - Alarmierung
  - Dokumentation
  - Detection & Prevention

snapSEC

Incident Response Plan

- Eindämmung
  - Sofort-Maßnahmen
  - System-Backup
  - Folge-Maßnahmen



snapSEC

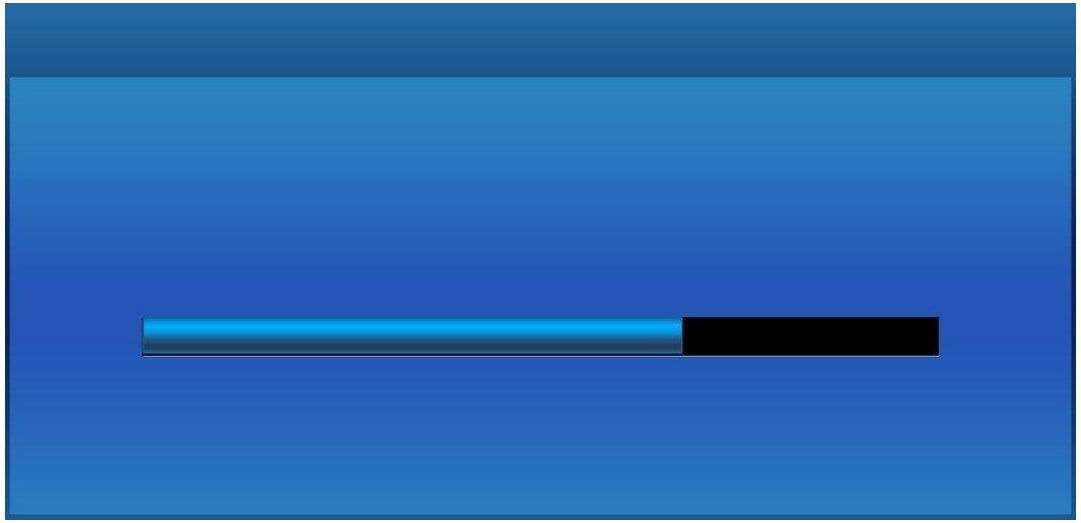
Incident Response Plan

- Beseitigung
  - Re-Imaging
  - Root-Cause Analyse
  - Anwendung Security Best Practices
  - Malware-/IoC-Scanning

snapSEC

Incident Response Plan

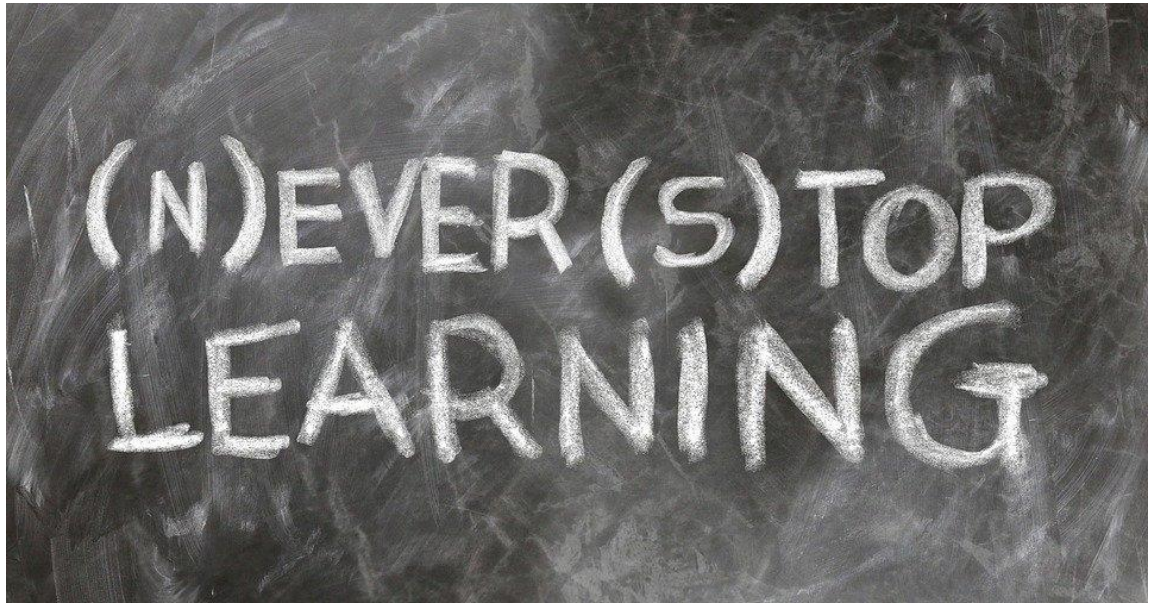
- Wiederherstellung
  - Definierung Zeitpunkt Wiederherstellung der Dienste
  - Prüfung und Verifizierung
  - Monitoring
  - Verhinderung weiterer Vorfälle



snapSEC

Incident Response Plan

- Lessons Learned
  - Finalisierung Dokumentation
  - Incident Reporting
  - Verbesserung Performance
  - Benchmarking
  - Lessons Learned Meeting



snapSEC

Incident Response Plan

HANDOUT

1) Definierung und Kommunikation Incident-Fallbeispiele (Datenverlust, Malwareausbruch, Phishing usw.)	*2) Installation Meldestelle für Incidents* (Helpdesk, Administratoren, Geschäftspartner, Security-Operation-Center,… 24/7 ja/nein?)	3) (Erst-)Dokumentation Incident-Meldung (Kontaktinformation der Person – die den Incident meldet, Zeitpunkt, Beschreibung des Incident, Unternehmensstandort, wie wurde der Incident entdeckt und wann ist dieser das erste Mal aufgefallen)
4) Kontaktierung Incident-Response Team/Management (Kontaktierung über Telefon/Mail, Personenbackup Adaptierung Incident-Meldung um geschätzten Business Impact, Beschreibung des Zielsystems und Informationen über Herkunft der Attacke)	*5) Ersteinschätzung durch Incident-Response Team* (Meeting oder Diskussion über Response-Strategie: worum handelt es sich bei dem Incident, was können mögliche Auswirkungen sein, ist der Angriff noch im Gange, welche Systeme/Daten/Lokationen sind betroffen, wie kritisch ist die Situation, Business Impact einer erfolgreichen Attacke – Critical/High/Low, wie viel Zeit bleibt/muss umgehend reagiert werden, welche Auswirkungen können die Reaktionen auf die Angreifer haben, Typ des Incidents – Malware, Backdoor, Ransomware,…)	*6) Kategorisierung des Incidents* (Bedrohung: - für die öffentliche Sicherheit - für sensible Daten - für Computer-Systeme - Störung/Beeinträchtigung von Services - …)
7) Course of Action (Response Prozeduren für Malwareausbruch, Systemausfälle, APT, Ransomware,…)	*8) Forensische Maßnahmen* (Review Security-Logs, IoC-Scanning, Befragung Betroffene, Root-Cause-Analyse,…)	*9) Vorkehrungen, um weitere Ausdämmung oder Neuinfektionen zu vermeiden* (Vorschläge durch Incident-Response Team, Implementierung nach Absegnung durch Management)
10) Disaster Recovery (Reimaging oder Restoring to unifected state, Passwort-Change, Service Hardening, Patching, EDR, Security-Monitoring,…)	*11) Update Incident-Dokumentation* (Incident-Discovery, -/Kategorie, -/Occurrence, -/Source, Course of Action, Effektivität, Aufbewahrung sämtl. (Forensik-)Logs und (Gesprächs-)Notizen,…)	*12) Meldung nach extern (wenn nötig)* (Data-Breach, Polizei, externe Partner, Tochtergesellschaften,…)
13) Bewertung des Schadens und Kosten für Incident Response und Disaster Recovery	*14) Lessons Learned* (Review Response, Update Policies/Response Plan/Course of Actions, Training, Cyber-Resilienz, was ist gut gelaufen/was kann man nächstes mal besser machen, Assessment Security Controls, standen ausreichend Ressourcen zur Verfügung – intern wie extern,…)	

snapSEC

Incident Response Plan

Sie haben Fragen?
Wir haben die Antworten!

hello@snapsec.at
+43-720-51-37-07

VORBEREITET ZU SEIN IST EINFACH, WENN MAN EINEN GUTEN PLAN HAT!

www.snapsec.at