Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/
Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: Hellwigstraße 8-10
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 47/2020

Datum: 11.09.2020

Checklisten zu Präventionsmaßnahmen

Protokollierung

Möchten Sie das Thema Cybersicherheit in Ihrem Unternehmen ernst nehmen? Hangeln Sie sich anhand dieser Checkliste durch die verschiedenen Themengebiete und prüfen Sie ob und wie Ihr Unternehmen aufgestellt ist.

Die Hinweise sind jeweils nicht abschließend, sondern decken nur die wichtigsten Bereiche der präventiven IT-Sicherheit ab.

Besprechen Sie die Hinweise und Fragen mit Ihrem IT-Dienstleister- bei entsprechender Kompetenz wird er auskunftsfähig sein und Ihre Fragen beantworten.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Polizei

SAARLAND

3. Protokollierung

Um in einem Fall des Angriffs eine Lokalisierung des Problems und eine schnelle Behebung durchführen zu können, empfiehlt sich das Führen von Protokolldateien bzw. Logfiles. Dabei muss im Vorfeld eine Abwägung zwischen der Menge an Logdateien und dem späteren Nutzen getroffen werden. Auch über das fortwährende Monitoring dieser Logdateien kann nachgedacht werden.

Beispiel:

Welche Benutzeraktionen sollen protokolliert werden? Wenig Sinn ergibt die Protokollierung auf Ebene von Dateioperationen (Anlegen, Löschen etc.) - eher sinnvoll ist die Protokollierung von administrativen Aktionen (Anlegen, Löschen von Benutzern) oder auch der eigentliche Anmeldevorgang an einem Client.

Jedes eingesetzte System hat seine eigenen Log-Modalitäten und Besonderheiten:

- Ein Router protokolliert nur solange wie er in Betrieb ist- nach einem Neustart sind die Protokolldaten verloren.
- Ein Mailserver protokolliert auf technischer Ebene die eingehenden und ausgehenden Mails (ohne Inhalt).
- Ein Webserver protokolliert auf IP-Ebene die eingehenden Verbindungen und die ausgelieferten Webseiten.
- Eine Firewall protokolliert u.U. die abgewiesenen Verbindungen.

Es besteht die Möglichkeit, Protokolldaten an einem zentralen Ort zusammenfließen zu lassen.

Das ergibt in einem nächsten Schritt die Möglichkeit, dass auf Basis der Protokollierung auch ein Warnsystem implementiert werden kann, so dass z.B. die fehlgeschlagenen Anmeldeversuche an einem Client oder dem Mailsystem an einen Administrator gemeldet werden.

Integrierbar in ein zentrales Warnsystem wäre auch die Prüfung auf eine mögliche Kompromittierung der Firmenwebseite.

Mit freundlichen Grüßen,

i.A.
Schmitt M.O.
Kriminalhauptkommissar

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken