

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- Hellwigstraße 8-10
gebäude: 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

Schulung der Mitarbeiter

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

© Mit freundlicher Genehmigung der ZAC Niedersachsen

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

1. Schulung der Mitarbeiter

Mitarbeiter (MA) sollten über die Gefahren im Zusammenhang mit IT und der täglichen Arbeit aufgeklärt werden. Mitarbeiter brauchen für Fragen im Zusammenhang mit IT einen festen, vertrauensvollen Ansprechpartner. MA sollten sensibilisiert werden, dass ungewöhnliche Vorfälle zeitnah an einen Verantwortlichen berichtet werden.

Mitarbeiter müssen darüber hinaus klare Regeln und Hinweise zur IT-Nutzung bekommen, dazu gehören z.B.

- Die zugelassene Art und Weise der Verwendung von privaten Komponenten (beispielsweise USB-Sticks) muss dargestellt werden.
- Die private Internetnutzung ist zu regeln und ggf. technisch zu reglementieren.
- Die Nutzung von privaten mobilen Endgeräten im Firmen-WLAN ist klar zu regeln bzw. zu unterbinden.
- Die Wichtigkeit eines guten Passwortes muss dargestellt werden.
- Die zugelassenen Datei-Endungen in der Unternehmenskommunikation sind festzulegen.
- Mitarbeiter müssen die Gefahren kennen, die beispielsweise durch Makros in Office-Dokumenten entstehen können.
- Es muss klar sein, dass ein installierter Virenschanner keinen absoluten Schutz vor Viren und Trojanern bietet.
- Die Abläufe und Verantwortlichen in der Firma in Sachen Administration und Wartung von IT-Komponenten müssen benannt werden.
- Der Ansprechpartner für technische Fragen oder ungewöhnliche Vorfälle muss bekannt sein und auch ansprechbar und hilfsbereit sein.
- Die Mitarbeiter sind auf Verschwiegenheitspflichten hinzuweisen.
- IT-gestützte Prozesse (bspw. die Art und Weise der Durchführung von Überweisungen) sind mit Nennung der Gefahren zu beschreiben.
- Eine Schulung hinsichtlich der Gefahren der unverschlüsselten und unsignierten Kommunikation via E-Mail ist notwendig, um den MA in die Lage zu versetzen, gefälschte E-Mailabsender oder manipulierte Ziel-Webseiten zu erkennen.
- Nutzen Sie ggf. Online-Seminare, die verpflichtend für alle Mitarbeiter angeboten werden, um den sicheren Umgang mit z.B. E-Mails zu vermitteln.

Mit freundlichen Grüßen,

i.A.
M.O. Schmitt

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