



Personalamt
Interne Kommunikation
interne-kommunikation@fd.so.ch

Cyber-Sicherheit: Intensivierung der Schulung und neue Massnahmen

Cyber-Sicherheit & Risiken

Das Thema Cyber-Sicherheit oder auch Informationssicherheit gewinnt stetig an Bedeutung. Cyber-Attacken prägen den heutigen Alltag und stellen somit ein grosses Risiko dar für die Sicherheit der Informationen und Geschäftsprozesse der Kantonalen Verwaltung.

Die Awareness, das Bewusstsein der Mitarbeitenden für den sicheren Umgang mit Daten und Informatikmitteln, ist daher von zentraler Wichtigkeit und muss stetig verbessert werden. Der Regierungsrat hat deshalb in seiner Sitzung vom 16. August 2022 ([Link zum RRB und Beilagen](#)) die nötigen Änderungen in der Weisung zu Nutzung und Abgabe von Informatikmitteln beschlossen.

Intensivierung der Schulung & Unterstützung der Mitarbeitenden

Zur Unterstützung aller Mitarbeitenden werden das AIO und das Personalamt die Schulungsmöglichkeiten weiter intensivieren und mithilfe eines Learning Management Systems (LMS) deutlich verbessern. Hinzu kommt die Weiterführung der Awareness-Kampagne mit fiktiven Phishing-Mails und diversen anderen Hilfestellungen (Informationen auf dem Intranet, Phishing-Button, etc.). Jedem Mitarbeitenden werden in einem Jahr maximal fünf Phishing-Mails mit verschiedenen Schwierigkeitsstufen versendet.

Damit die Sicherheit unserer Informationen und Systeme gegen neueste Gefahren stets gewährleistet ist, ist es wichtig, Mitarbeitende, welche sich im Rahmen der Awareness-Kampagne wiederholt falsch verhalten, zu kennen um sie unterstützen zu können. Mitarbeitende verhalten sich falsch, wenn sie eine Phishing-Mail öffnen, auf einen Link, einen Button oder eine Beilage im E-Mail klicken, und **zusätzlich**

- User-ID oder E-Mail-Adresse und Passwort auf einer Webseite eingeben, oder
- einen Download von Schadsoftware nach einer aktiven Bestätigung durchführen, oder
- die einer E-Mail als Anhang beigefügte Datei öffnen und die Makro- bzw. eine Sicherheitswarnung übersteuern.

Mitarbeitende, die sich ein erstes Mal falsch verhalten, werden automatisiert informiert. Im Wiederholungsfall in einem Zeitraum von weniger als 12 Monaten, erfolgt durch unseren externen Awareness-Partner eine Meldung an das Personalamt, so dass geeignete Schulungs- und Sensibilisierungsmassnahmen für die jeweiligen Benutzer eingeleitet

werden können. Ab einem dritten falschen Verhalten, erfolgt eine Information an die Vorgesetzten in Verbindung mit einer spezifischen Schulung resp. Sensibilisierung. Erfolgt während den 12 Monaten kein weiterer Vorfall, werden die aufgezeichneten Daten gelöscht und das geschilderte Vorgehen beginnt von neuem.

Weitere Änderungen

Die Weisung zu Nutzung und Abgabe von Informatikmitteln wird ebenfalls in folgenden weiteren Punkten ergänzt:

- Die Weisung gilt neu auch für die Mitarbeitenden der Polizei Kanton Solothurn, unter Berücksichtigung der polizeilichen Besonderheiten.
- Weil bei einem echten und geglückten Cyberangriff schnell reagiert werden muss, können Mitarbeitende, die Opfer eines echten Cyberangriffs wurden, sofort und namentlich identifiziert werden.
- Neu stellt auch die grobfahrlässige oder vorsätzliche Missachtung von Sicherheitsvorkehrungen eine missbräuchliche Nutzung dar, die nach Verantwortlichkeitsgesetz oder Staatspersonalgesetz sanktioniert werden kann.
- Die Weisung zeigt das Verfahren auf, wie bei der fristlosen Auflösung des Anstellungsverhältnisses oder bei Freistellung eines Mitarbeitenden auf dringend benötigte geschäftliche Daten zugegriffen werden kann und wie in diesen Fällen mit den privaten Daten zu verfahren ist.

Die Änderungen treten am 1. September 2022 in Kraft.

Die Einführung dieser Massnahmen ist zum Schutz der Kantonalen Verwaltung vor Cyber-Attacken unverzichtbar.

Weitere Auskünfte:

Toni Widmer, Leiter Informationssicherheit/QS, Amt für Informatik und Organisation,
032 627 23 26

SO pin 22-17
12.09.2022