KANTON solothurn

Regierungsratsbeschluss

vom 16. August 2022

Nr. 2022/1198

Weiterentwicklung der Weisung zu Nutzung und Abgabe von Informatikmitteln

1. Ausgangslage

Cyber-Risiken prägen den heutigen Alltag. Für Aufsehen sorgen immer wieder breit angelegte Angriffswellen, die weltweit zu grossen Schäden führen. Cyber-Attacken stellen auch ein grosses Risiko dar für die Sicherheit der IT, der Daten und Geschäftsprozesse der Kantonalen Verwaltung und müssen ernst genommen werden.

Die jetzige Situation bezüglich Informationssicherheit und Sicherheit der Informatiksysteme ist unbefriedigend. Die Auswertung der Awareness-Kampagne **denk**vor**klick** 2021 zeigt, dass in den Bereichen E-Mail Phishing und WebInfection rund 9.9 % (= 342 Mitarbeitende) den Angriff nicht erkannten und auf den Link klickten. Rund 8.3 % (= 286 Mitarbeitende) haben sich auf den gefälschten Webseiten falsch verhalten, ihren Benutzernamen sowie ihr Passwort eingegeben oder Software installiert. Das Fehlverhalten von fast 300 Mitarbeitenden ist zu hoch und stellt eine zu grosse Gefahr dar für die Informationssicherheit und die Informatiksysteme der kantonalen Verwaltung. Die Auswertung hat weiter ergeben, dass im Jahr 2021 17 Mitarbeitende mehrfach, d.h. zwei oder mehrere Male, auf die Angriffsmuster hereingefallen sind.

Es ist davon auszugehen, dass die Sensibilisierung in Bezug auf solche Angriffe immer noch unzureichend ist, nicht die gewünschte Wirkung erzielt hat und dass es offensichtlich immer noch zu viele Mitarbeitende mit einem Informations- und Verhaltensdefizit gibt. Zu denken gibt insbesondere die Anzahl derjenigen Mitarbeitenden, die mehrfach falsch geklickt haben. Diese sollen namentlich ausfindig gemacht und gezielt geschult werden. Die personenbezogene Auswertung von Protokolldaten soll das ermöglichen. Mit diesem Beschluss wird die dafür notwendige Rechtsgrundlage in der Weisung zu Nutzung und Abgabe von Informatikmitteln (RRB Nr. 2018/1864 vom 27. November 2018) geschaffen.

Die Weisung wird zudem in folgenden weiteren Punkten ergänzt: Sie macht die personenbezogene Auswertung von Protokolldaten auch in den Fällen möglich, wo Benutzer Opfer eines echten Cyberangriffs werden. In diesen Fällen kann das Amt für Informatik und Organisation sofort die Protokolldaten personenbezogen auswerten. Weiter wird neu festgehalten, dass auch die grobfahrlässige oder vorsätzliche Missachtung von Sicherheitsvorkehrungen eine missbräuchliche Nutzung darstellen, die nach Verantwortlichkeitsgesetz oder Staatspersonalgesetz sanktioniert werden kann. Schliesslich regelt die Weisung neu, dass auch bei Beendigung des Anstellungsverhältnisses sowie im Fall der Freistellung eines Benutzers auf dringend benötigte geschäftliche Daten zugegriffen werden kann und, wie im Fall der Freistellung oder fristlosen Auflösung des Anstellungsverhältnisses mit den privaten Daten der Mitarbeitenden zu verfahren ist.

Neu soll auch die Polizei Kanton Solothurn (Polizei) vom Geltungsbereich der Weisung erfasst sein, unter Berücksichtigung der polizeilichen Besonderheiten.

2. Personenbezogene Auswertung von Protokolldaten

Was sind Protokolldaten? Beim Surfen oder Mailen hinterlassen Benutzer auf ihren Informatikmitteln Spuren, die durchgeführten Aktivitäten werden protokolliert in den Protokolldaten. Es ist technisch möglich, diese Daten personenbezogen auszuwerten, missbräuchliches Verhalten eines Benutzers aufzudecken oder schädigende Handlungen einem konkreten Benutzer zuzuordnen.

2.1 Bestehende Regelung zur personenbezogenen Auswertung von Protokolldaten

Die Weisung zu Nutzung und Abgabe von Informatikmitteln lässt die personenbezogene Auswertung von Protokolldaten nur zu bei einem begründeten Verdacht auf eine missbräuchliche Nutzung von Informatikmitteln (Ziffer 21 und 26). Diese Fälle lassen auch Sanktionen zu, weil die missbräuchliche Nutzung eine Verletzung von Dienstpflichten darstellt, welche sanktioniert werden kann nach Staatspersonal- und Verantwortlichkeitsgesetz (Ziffer 22).

Wird aber aus Nachlässigkeit und Unkenntnis falsch geklickt, hat das Amt für Informatik und Organisation (AIO) aufgrund der bestehenden Regelung keine Möglichkeit, die Namen der betroffenen Mitarbeitenden in Erfahrung zu bringen und diese gezielt zu schulen. Bei Awareness-Kampagnen mit fiktiven Phishing-Mails ist die personenbezogene Auswertung der Protokolldaten nicht möglich.

2.2 Voraussetzungen zur personenbezogenen Auswertung von Protokolldaten

Aufzeichnen und personenbezogenes Auswerten von Protokolldaten stellen eine Bearbeitung von Personendaten im Sinn von § 6 Absatz 5 des Informations- und Datenschutzgesetzes vom 21. Februar 2001 (InfoDG; BGS 114.1) dar, die eine Rechtsgrundlage gemäss § 15 InfoDG benötigt und nebst anderen den allgemeinen Grundsätzen des Datenschutzrechts genügen muss, wie der Verhältnismässigkeit, dem Handeln nach Treu und Glauben und der Zweckbindung (§ 16 InfoDG).

Die Rechtsgrundlage für Aufzeichnen und Auswerten von Protokolldaten findet sich in der Weisung zu Nutzung und Abgabe von Informatikmitteln. Es ist sachlogisch, diese Weisung zu ergänzen bezüglich der Aufzeichnung und weitergehenden personenbezogenen Auswertung von Protokolldaten. Da fiktive Phishing-Angriffe keine echte Gefahr darstellen und nur den Ernstfall proben, hat die Aufzeichnung und personenbezogene Auswertung von Protokolldaten in diesen Fällen zumindest erhöhten Anforderungen zu genügen. Eine Überwachung darf erst dann in Erwägung gezogen werden, wenn die Mitarbeitenden regelmässig genügend geschult und sensibilisiert worden sind und diese Massnahmen nicht genügen, das Risiko für die kantonale Verwaltung tragbar zu machen. Bevor die personenbezogene Auswertung von Protokolldaten überhaupt in Frage kommt, müssen demnach aus Gründen der Verhältnismässigkeit zuerst alle anderen möglichen Massnahmen technischer und schulischer Natur zum Schutz der Informatikmittel und Daten ausgeschöpft worden sein. Schulung und Sensibilisierung geht vor Überwachen. Aufzeichnen und Auswerten der Protokolldaten dürfen weiter nur zum gesetzlich vorgesehenen Zweck erfolgen, und die Benutzer sind über die geltenden Bestimmungen aufzuklären.

3. Intensivierung der Sensibilisierung

Ziel ist es, das Bewusstsein jedes einzelnen Mitarbeitenden für die Sicherheit im Umgang mit den Informatikmitteln und den Daten seines Arbeitgebers zu steigern, ihn für Themen rund um die IT-Sicherheit zu sensibilisieren und ihm unterschiedliche Sicherheitsbedrohungen in seiner alltäglichen Arbeit aufzuzeigen. Jeder einzelne Mitarbeitende soll erkennen, dass Sicherheit von IT und Daten nicht nur Sache der IT-Abteilung und des Datenschutzes ist, sondern alle und jeden angeht.

Das AIO schafft mit den bereits vorhandenen Sicherheitsmassnahmen, die den Gefahren der virtuellen Welt angepasst sind (IKT-Grundschutz, Authentifizierung und Autorisierung, Verschlüsselungsanwendungen, Antivirenprogramme, Disquotmanager, Backups und Firewalls), die nötige technische Voraussetzung um Cyber-Angriffe erfolgreich abzuwenden. Den Mitarbeitenden wird neu die Möglichkeit gegeben, verdächtige E-Mails im Outlook über einen Phishing Response Service kontrollieren zu lassen. Das AIO wird die Awarenessmassnahmen weiter intensivieren. Mit der Einführung eines Learning Management Systems, das nicht nur zur Awareness-Schulung eingesetzt werden kann, soll das erreicht werden. Mitarbeitende sollen befähigt werden, Angriffe zu erkennen und sich richtig zu verhalten und so dazu beitragen, das Risiko für erfolgreiche tatsächliche Cyberangriffe auf die kantonale Verwaltung zu minimieren.

Insbesondere diese Intensivierung von Massnahmen zur Sensibilisierung macht die Erweiterung des Geltungsbereichs der Weisung auch für die Polizei sachgerecht und verfahrensökonomisch sinnvoll.

4. Personenbezogene Auswertung von Protokolldaten bei wiederholtem Fehlverhalten

Zur Schulung hinzu kommt die Weiterführung der Awarenessmassnahmen mit fiktiven Phishing-Angriffen. Mit dem Versand von fiktiven Phishing-Mails, die exakt dem Vorgehen von Cyberkriminellen entsprechen und den Ernstfall proben, soll das Verhalten der Mitarbeitenden im Umgang mit echten Angriffen sensibilisiert und nachhaltig verbessert werden.

An jeden Mitarbeitenden werden in zwölf Monaten maximal fünf fiktive Phishing-Mails (mit verschiedenen Schwierigkeitsstufen) versandt. Erwartet wird, dass Mitarbeitende diese Mails als Cyberangriff erkennen, löschen oder mit dem Phishing-Button überprüfen lassen. Bei einem Fehlverhalten wird der Mitarbeitende umgehend automatisiert informiert, es werden die wichtigsten Tipps zur Erkennung solcher Angriffe nochmals in Erinnerung gerufen. Bei einem Fehlverhalten werden die aufgezeichneten Protokolldaten während zwölf Monaten aufbewahrt und dann gelöscht, wenn sich in dieser Zeit kein weiteres Fehlverhalten ereignet. Wird der Mitarbeitende in dieser Zeit allerdings ein weiteres Mal Opfer einer fiktiven Phishing-Mail, lässt dies darauf schliessen, dass der Mitarbeitende ungenügend sensibilisiert ist, zusätzliche Unterstützung braucht und intensiver geschult werden muss. Der externe Awareness-Anbieter übermittelt in diesen Fällen dem Personalamt die Ergebnisse der personenbezogen ausgewerteten Protokolldaten und gibt damit die Person des betroffenen Mitarbeitenden bekannt. Das Personalamt prüft die geeigneten Schulungs- und Sensibilisierungsmassnahmen. Bei einem dritten und jedem weiteren Fehlverhalten innert zwölf Monaten seit dem letzten Fehlverhalten wird der Benutzer wieder automatisiert über sein Fehlverhalten informiert, der Awareness-Anbieter übermittelt die Ergebnisse der personenbezogen ausgewerteten Protokolldaten dem Personalamt, welches die geeigneten Schulungs- bzw. Sensibilisierungsmassnahmen bestimmt und informiert, falls dies für Schulung und Sensibilisierung erforderlich ist, die vorgesetzte Person. Kommt es während zwölf Monaten zu keinem weiteren Fehlverhalten, werden die Protokolldaten gelöscht und das in nachfolgender Übersicht aufgezeigte mehrstufige Vorgehen beginnt wieder von neuem.

Zur Übermittlung der Namen der fehlbaren Benutzer ans Personalamt kommt es also erst bei einem zweiten und jedem weiteren Fehlverhalten innert zwölf Monaten seit dem letzten Fehlverhalten. Die vorgesetzte Person wird ab dem dritten Fehlverhalten (innert zwölf Monate seit dem letzten Fehlverhalten) informiert, sofern es angezeigt ist zur Schulung und Sensibilisierung des Mitarbeitenden.

Mehrstufiges Vorgehen

1. Fehlverhalten	– Automatisierte Information bzgl. Fehlverhalten und spezifischem Problem
2. Fehlverhalten	– Automatisierte Information bzgl. Fehlverhalten und spezifischem Problem – Mitteilung an das Personalamt – Personalamt bestimmt geeignete Schulung
3. und jedes weitere Fehlverhalten	– Automatisierte Information bzgl. Fehlverhalten und spezifischem Problem – Mitteilung an das Personalamt – Personalamt bestimmt geeignete Schulung – Personalamt informiert, soweit erforderlich, die vorgesetzte Person

Ein Fehlverhalten im Sinn der Weisung liegt dann vor, wenn eine Phishing-Mail geöffnet und auf einen Link, einen Button oder eine Beilage im E-Mail geklickt wird und zusätzlich

- User-ID oder E-Mail-Adresse und Passwort auf einer Webseite eingegeben werden, oder
- ein Download von Schadsoftware nach einer aktiven Bestätigung durchgeführt wird, oder
- die einer E-Mail als Anhang beigefügte Datei geöffnet und die Makro- bzw. eine Sicherheitswarnung übersteuert wird.

5. Erläuterungen zu den Bestimmungen

Ziffer 2
Die Polizei war bislang vom Geltungsbereich der Weisung zu Nutzung und Abgabe von Informatikmitteln ausgenommen. Die Gründe dafür lagen in der weitestgehend unabhängigen IT-Infrastruktur der Polizei und in der Nutzung verschiedener polizeispezifischer Informationstechnologien. Dienstleistungen im IT-Bereich der Polizei werden seit jeher nicht vom AIO, sondern von einem polizeiinternen Fachdienst (Technischer Führungsdienst, TFD) selbständig erbracht. Die beiden Ämter sind technisch durch ein Netzwerk miteinander verbunden. Das AIO hat keinen Zugriff auf die Server, die Arbeitsplatzsysteme und die Protokolldaten der Mitarbeitenden der Polizei. Ebenfalls obliegt es dem TFD, den sicheren Fernzugriff für die Mitarbeitenden der Polizei zu gewährleisten. Diese Strukturen und Verantwortlichkeiten haben sich bewährt, weshalb nicht alle Bestimmungen der Weisung ohne Weiteres auf die Polizei anwendbar sind. Macht die zum Schutz der polizeilichen Aufgabenerfüllung bestehende technische Autonomie eine abweichende Bestimmung nötig, wird dies in der Weisung in den entsprechenden Bestimmungen erwähnt.

Ziffer 3
Aufgrund der Ausdehnung des Geltungsbereichs für die Polizei ist Buchstabe c zu ergänzen: Leistungserbringer der Polizei ist der Technische Führungsdienst (TFD). In Buchstabe h werden der Vollständigkeit halber die Monitore angeführt. Wegen den in diesem Beschluss vorgenommenen Änderungen werden in den Buchstaben k – n folgende neue Begriffe definiert: Awareness, Phishing-Mail, Schadsoftware sowie Makro-/Sicherheitswarnung.

Ziffer 11
Für die Mitarbeitenden der Polizei gelten bei Verlust und Diebstahl von Informatikmitteln spezifische Richtlinien des Polizeikommandos.

Ziffer 13
Mit RRB Nr. 2017/1744 vom 23. Oktober 2017 wurde die Weisung zur Aufbewahrung von E-Mails in der kantonalen Verwaltung beschlossen. Die Polizei ist vom Geltungsbereich dieser Weisung ausgenommen. Wie bis anhin gilt für die Mitarbeitenden der Polizei die Weisung des Polizeikommandos.

Ziffer 16
Diese Bestimmung regelt den Zugriff auf dringend benötigte geschäftliche Daten eines Benutzers, ohne dass seine Zustimmung eingeholt werden kann. Dies soll nicht nur bei unvorhergesehener Abwesenheit, sondern neu auch bei der Beendigung des Anstellungsverhältnisses und bei Freistellung möglich sein.

Ziffer 17
Neu wird in dieser Bestimmung das Verfahren geregelt, wie die Benutzer im Fall der Freistellung und der fristlosen Auflösung des Anstellungsverhältnisses Zugriff auf ihre privaten Daten erhalten.

Ziffern 18 – 19
Gestützt auf die bestehenden Richtlinien des Polizeikommandos nehmen Polizistinnen und Polizisten verschiedene Tätigkeiten an Ort und Stelle mittels Smartphone und/oder Client Gerät vor. Unter Berücksichtigung der besonderen Sensibilität der bearbeiteten Personendaten gelten für polizeiliche Daten teilweise strengere Schutzmassnahmen. Auch unterliegt die polizeiliche Datenbearbeitung im Vergleich zur übrigen Verwaltung weitergehenden Kontrollmechanismen. Ergänzend zu den Richtlinien des AIO gelten deshalb für die Mitarbeitenden der Polizei die entsprechenden Richtlinien des Polizeikommandos. Die Richtlinien gewährleisten die Informationssicherheit, wahren die Persönlichkeitsrechte der Betroffenen, haben sich bewährt und sollen weiterhin zur Anwendung gelangen. Dies gilt auch für die Richtlinien des Polizeikommandos zu mobilen Datenträgern.

Ziffer 20
Den Mitarbeitenden der Polizei ist es gemäss den geltenden Richtlinien des Polizeikommandos grundsätzlich untersagt, zur Verrichtung einer dienstlichen Tätigkeit das privat beschaffte Mobiltelefon oder Smartphone zu benutzen, weshalb Ziffer 20 nicht gilt für die Mitarbeitenden der Polizei.

Ziffer 21
Diese Bestimmung definiert die missbräuchliche Nutzung von Informatikmitteln.

Buchstabe b
Zu den gesetzlichen Aufgaben der Mitarbeitenden der Polizei (insbesondere Cybercops, Fahnder und Ermittler) gehört es unter anderem, auf Datenträgern Hinweisen auf strafbares Verhalten (z.B. Rassendiskriminierung, verbotene Pornografie) nachzugehen, beziehungsweise auf einschlägigen Websites und Foren entsprechende Abklärungen und Ermittlungen zu tätigen. Im

Rahmen von Dienstpflichten ist es für Mitarbeitende der Polizei demzufolge regelmässig unerlässlich, auf Daten i.S. von Buchstabe b zuzugreifen. Was den Mitarbeitenden der übrigen Verwaltung grundsätzlich untersagt ist und als missbräuchliche Nutzung entsprechende Folgen nach sich zieht, kann bei Mitarbeitenden der Polizei eine gesetzlich und dienstlich erforderliche Amtspflicht darstellen. Um die polizeiliche Aufgabenerfüllung nicht zu erschweren, gilt für die Mitarbeitenden der Polizei deshalb die (widerlegbare) Vermutung, dass der konkrete Zugriff im Rahmen eines dienstlichen Auftrags sowie im Einverständnis des Polizeikommandos erfolgt ist.

In einem neuen Absatz wird die missbräuchliche Nutzung mit einem neuen Tatbestand ergänzt: Auch die vorsätzliche oder grobfahrlässige Missachtung von Sicherheitsvorgaben stellt eine missbräuchliche Nutzung dar, welche gemäss Ziffer 26 die personenbezogene Auswertung von Protokolldaten erlaubt und gemäss Ziffer 22 eine Sanktionierung nach dem Staatspersonalgesetz und dem Verantwortlichkeitsgesetz zulässt.

Ziffer 22
Der Polizeikommandant entscheidet über den Entzug von Informatikmitteln oder der Zugangsberechtigung auf ein Informatikmittel auf Antrag des TFD.

Titel vor Ziffer 23
Verantwortlich für Schutz, Überwachung und Kontrollen gemäss den Ziffern 23 – 26 ist der jeweilige Leistungserbringer.

Leistungserbringer für die Polizei ist der TFD, welcher wie bis anhin zuständig bleibt für die technischen Schutzmassnahmen (Ziffer 23), die Protokollierung (Ziffer 24) sowie die Auswertung von Protokolldaten der Mitarbeitenden der Polizei, soweit diese nicht im Rahmen einer Awareness-Kampagne gemäss Ziffer 26 Absatz 2 Buchstabe b erfolgt. Im Zusammenhang mit einer Awareness-Kampagne nimmt das AIO, resp. der externe Awareness-Anbieter, die anonyme Auswertung der Protokolldaten vor (Ziffer 25). Die Polizei liefert dem AIO die dazu erforderlichen E-Mail-Accounts der Mitarbeitenden der Polizei.

Ziffer 24
Voraussetzung zur personenbezogenen Auswertung von Protokolldaten ist deren Protokollierung. Diese soll in den Fällen von Ziffer 26 möglich sein.

Ziffer 25
Das AIO kann nicht auf die Protokolldaten der Mitarbeitenden der Polizei zugreifen. Die anonyme Auswertung der Protokolldaten nimmt darum jeder Leistungserbringer selber vor. Zur anonymen Auswertung von Protokolldaten im Zusammenhang mit Awareness überlässt die Polizei dem AIO auf Anfrage die hierfür nötigen E-Mail-Accounts der Mitarbeitenden der Polizei.

Ziffer 26
Die bestehende Ziffer 26 nennt die Voraussetzungen zur personenbezogenen Auswertung von Protokolldaten durch das AIO beziehungsweise durch den TFD. Neu soll dies nicht nur möglich sein bei einem begründeten Verdacht auf eine missbräuchliche Nutzung von Informatikmitteln im Sinn von Ziffer 21.

Der neue Absatz lässt in Buchstabe a die personenbezogene Auswertung von Protokolldaten auch zu bei einer ernsthaften und konkreten Gefährdung der Sicherheit und Verfügbarkeit der Informatikmittel und der Daten der kantonalen Verwaltung. Die personenbezogene Auswertung von Protokolldaten durch das AIO beziehungsweise durch den TFD soll die Identifizierung derjenigen Personen ermöglichen, die Opfer eines echten und erfolgreichen Cyberangriffs wurden.

Buchstabe b lässt zu Schulungs- und Sensibilisierungszwecken die Identifizierung derjenigen Personen zu, die sich wiederholt falsch verhalten haben im Rahmen einer Awareness-Kampagne.

Namentlich identifiziert werden die Personen, denen im Abstand von weniger als zwölf Monaten seit dem letzten Fehlverhalten ein weiteres Fehlverhalten unterläuft. Der externe Awareness-Anbieter gibt in diesen Fällen dem Personalamt die Namen der betroffenen Mitarbeitenden bekannt. Das Personalamt bestimmt die geeigneten Schulungs- und Sensibilisierungsmassnahmen. Auch bei einem dritten und jedem weiteren Fehlverhalten innert zwölf Monaten seit dem letzten Fehlverhalten wird die Schulung intensiviert. Zusätzlich wird ab dem dritten Fehlverhalten die vorgesetzte Person informiert, sofern dies Sensibilisierung und Schulung erforderlich machen. Mit dem Ziel der Erhöhung der Awareness gilt die Bestimmung vollumfänglich auch für die Mittarbeitenden der Polizei.

6. Inkrafttreten

Die Änderungen der Weisung zu Nutzung und Abgabe von Informatikmitteln (RRB Nr. 2018/1864 vom 27. November 2018) treten nach dem Beschluss des Regierungsrates am 1. September 2022 in Kraft.

7. Beschluss

7.1 Die Änderungen der Weisung zu Nutzung und Abgabe von Informatikmitteln (RRB Nr. 2018/1864 vom 27. November 2018) werden beschlossen.

7.2 Die Änderungen treten am 1. September 2022 in Kraft.

Andreas Eng
Staatsschreiber

Beilage

Weisung zu Nutzung und Abgabe von Informatikmitteln
Synopse

Verteiler

Beauftragte für Information und Datenschutz
Informatik Gruppe Verwaltung (7, Versand durch AIO)
Departemente und Staatskanzlei (6)
Ämter (42)