Medieninformation

Sächsischer Datenschutzbeauftragter

Ihr Ansprechpartner
Andreas Schneider

Durchwahl
Telefon 0351/85471-120
Telefax 0351/85471-109

saechsdsb@
slt.sachsen.de*

Aktenzeichen
SPR-0121/11/52

Dresden,
5. November 2021

Digitalisierung sicher gestalten:
Mehr Schutz vor Cyberattacken notwendig

- Sachsens Datenschutzbeauftragter plädiert für mehr Prävention.
- Jeder Cyberangriff kostet im Schnitt mehr als 21.000 Euro.

Angesichts der jüngsten Hacker-Angriffe gegen deutsche Unternehmen plädiert der Sächsische Datenschutzbeauftragte für deutlich mehr Prävention. "Sachsens Unternehmen sollten nicht erst warten, bis sie das Opfer von Hacker-Attacken geworden sind", sagt Andreas Schurig. Im Gegenteil: "Prävention ist wirksamer und wichtiger als je zuvor, damit Daten von Kunden und Mitarbeitern nicht in die falschen Hände gelangen."

Zuwachs bei gemeldeten Datenpannen

Nach der Datenschutz-Grundverordnung müssen Unternehmen genauso wie Organisationen und die Verwaltung Datenschutzverletzungen bei der zuständigen Aufsichtsbehörde melden. Der Trend in Sachsen zeigt hierbei deutlich nach oben: Im Jahr 2018 meldeten Verantwortliche dem Sächsischen Datenschutzbeauftragten 227 Fälle. 2019 waren es 450 Meldungen. 2020 verzeichnete die Behörde einen Anstieg um 40 Prozent auf 635 Meldungen. Und diese kontinuierliche Steigerung setzt sich 2021 fort: In den vergangenen zehn Monaten wurden bereits 750 Meldungen registriert. Davon sind rund ein Drittel auf Cyberkriminalität zurückzuführen – ein spürbarer Zuwachs in der Arbeit des Sächsischen Datenschutzbeauftragten. „Allerdings gehe ich davon aus, dass es in Wirklichkeit viel mehr Betroffene gibt. Die Dunkelziffer dürfte sehr hoch sein“, sagt Andreas Schurig. Und diese Hacker-Angriffe sind für die betroffenen Unternehmen und Organisationen teuer: Eine Cyberattacke kostet im Schnitt 21.818 EUR je Vorfall (Quelle: Statista). Die Zahl der Angriffe und das Ausmaß der Schäden nehmen stark zu. Insgesamt belaufen sich die

Hausanschrift:
Sächsischer Datenschutzbeauftragter
Devrientstraße 5
01067 Dresden

www.saechsdsb.de

Verkehrsanbindung:
Zu erreichen mit der Straßenbahnlinie 4
(Haltestelle Am Zwingerteich)

*Informationen über die Verarbeitung Ihrer personenbezogenen Daten und zum Zugang für verschlüsselte E-Mails finden Sie unter https://www.saechsdsb.de/Datenschutzerklaerung.

Kosten für digitale Angriffe auf die deutsche Wirtschaft allein 2020 auf ca. 24,3 Milliarden Euro. Das waren viermal mehr als noch 2019 (Quelle: Bitkom-Studie).
Noch gravierender sind durch Erpressungssoftware (engl. “Ransomware”) verursachte Schäden: Die durchschnittlichen Gesamtkosten der Firmen für die Behebung eines Angriffs durch Erpressungssoftware liegen bei ca. einer Million Euro; etwa 46 Prozent der deutschen Unternehmen sind betroffen (Quelle: Sophos State of Ransomware 2021).
“Diese Entwicklung ist sehr besorgniserregend. Mangelhafte Datensicherheit offenbart meist auch Schwächen beim Datenschutz. Das ist nicht nur für die betroffenen Unternehmen existenzbedrohend, sondern auch für Menschen, deren Daten in den Besitz von Kriminellen gelangen. Identitätsdiebstahl gehört dabei zu den schlimmsten Folgen. Betroffenen droht ein finanzieller und sozialer Totalschaden“, warnt Andreas Schurig.

Vorsorge bestes Mittel

Gleichzeitig macht der oberste sächsische Datenschützer klar, dass Prävention und Vorsorge die richtigen Mittel gegen Hacker-Angriffe und Cyber-Erpressung sind. „Der beste Schutz ist, auf den Ernstfall gut vorbereitet zu sein.“ Folgende Vorkehrungen sind zu empfehlen:

- **Daten sichern!** Die Daten von Firmen und Organisationen müssen unbedingt gesichert sein. Diese Backups sollten selbst nicht von Cyberangriffen erfasst werden können.
- **Firewall richtig konfigurieren!** Die Firewall sollte nur erforderliche Datenverbindungen zulassen. Auch ein Frühwarnsystem über ungewöhnlich hohen Datenverkehr kann Systemverantwortlichen dabei helfen, größeren Schaden abzwenden.
- **Notfallplan beachten!** Für die Fälle von Cyber-Erpressungen bzw. Hacker-Angriffen sollte ein Notfallplan vorliegen, der im Akutfall abzuarbeiten ist. Dazu gehört auch eine Regelung, wann der IT-Administrator, Datenschutzbeauftragte oder auch die Mitarbeiter, Unternehmensleitung und Kunden zu informieren sind.
- **Reservetechnik vorhalten!** Eine dringende Empfehlung ist zudem, Reservetechnik vorzuhalten. Ermittler können das angegriffene IT-System forensisch untersuchen, während das Unternehmen trotz Cyberangriff rasch wieder arbeitsfähig ist.

- **Frühzeitig kommunizieren!** Verantwortliche sollten betroffene Personen oder Abteilungen auch dann schnell über den Vorfall informieren, wenn noch nicht sicher ist, ob und welche personenbezogenen Daten betroffen sind.
- **Weiterbildung**! IT-Verantwortliche und all jene, die in Unternehmen und Organisationen für die IT-Sicherheit zuständig sind, benötigen regelmäßig Weiterbildungen.

"Prävention ist eine richtige und kluge Investition, die sich im Fall einer Attacke erheblich auszahlt", sagt Sachsens Datenschutzbeauftragter Andreas Schurig. Die Alternative zu Prävention sei bei Cyber-Erpressung oftmals nur der teure Freikauf.

Anzeige und Meldung bei der zuständigen Datenschutzbehörde

Im Falle einer Verletzung des Schutzes personenbezogener Daten hat der Verantwortliche gemäß Artikel 33 der Datenschutz-Grundverordnung unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, dies dem Sächsischen Datenschutzbeauftragten zu melden. Dazu bietet die Behörde auf ihrer Website ein Online-Formular an, mit dem die Verantwortlichen alle relevanten Informationen schnell und unkompliziert übermitteln können.

Welche Informationen benötigt der Sächsische Datenschutzbeauftragte?

Bei einem Hackerangriff, Datendiebstahl oder anderen Attacken sollten Unternehmen bzw. Verantwortliche sich so schnell wie möglich bei der Polizei melden. Parallel sollte die Datenschutzverletzung dem Sächsischen Datenschutzbeauftragten mitgeteilt werden. Wichtige Angaben für eine solche Meldung nach Artikel 33 Datenschutz-Grundverordnung sind:

- Angaben zum Verantwortlichen (Name des betroffenen Unternehmens/Vereins etc.) inkl. Telefon- und E-Mail-Kontakt;
- Zeitraum der Panne sowie Zeitpunkt des Vorfalls;
- Angaben zu Bereich und Kategorie des Vorfalls (z. B. Hacking, Diebstahl usw.);
- Angaben zu betroffenen Daten (z. B. Adressen, E-Mail-Adressen, Bank- oder Kreditdaten, Passwörter, Gesundheit)
- Angaben zum Vorfall und zu den ergriffenen und/oder beabsichtigten Maßnahmen.

Auf die Meldung der Datenpanne folgt die Prüfung durch den Sächsischen Datenschutzbeauftragten. Hierbei ist vor allem von Interesse: Welcher Schaden könnte Personen durch den Vorfall entstehen bzw. welcher Schaden ist bereits eingetreten? Wie konnte es dazu kommen und welche Vorkehrungen sind zukünftig zur Vermeidung einer Wiederholung zu ergreifen? Sofern erforderlich, steht der Sächsische Datenschutzbeauftragte bei der Klärung dieser Fragen mit dem Verantwortlichen im Austausch und berät bei den zu ergreifenden Maßnahmen. Das Ziel ist stets, Bürgerinnen und Bürger bei hohen Risiken zu informieren und sie durch die richtigen Maßnahmen vor Schaden zu bewahren.

Über den Sächsischen Datenschutzbeauftragten

Der Sächsische Datenschutzbeauftragte ist für Sachsen die unabhängige Datenschutz-Aufsichtsbehörde nach Artikel 51 Absatz 1 der Datenschutz-Grundverordnung (DSGVO). Dies ergibt sich im Hinblick auf nicht-öffentliche Stellen (z. B. Unternehmen und Vereine) aus § 14 Absatz 2 des Sächsischen Datenschutzdurchführungsgesetzes; im Hinblick auf öffentliche Stellen (z. B. Behörden) aus § 14 Absatz 1 desselben Gesetzes.

Seit 2004 hat Andreas Schurig das Amt inne und wird in seiner Dienststelle in Dresden von über 30 Mitarbeiterinnen und Mitarbeitern unterstützt. Der Sächsische Datenschutzbeauftragte kontrolliert die Einhaltung der Datenschutzvorschriften und geht Beschwerden von Bürgerinnen und Bürgern nach. Zu den weiteren Aufgaben zählt unter anderem die Beratung sächsischer Verantwortlicher bei datenschutzrechtlichen Fragestellungen.

Mehr Informationen: www.saechsdsb.de