Informationsblatt

Ransomware-Präventionsprüfung

Stand: 30.11.2021

Rechtliche Grundlage zur Onlineprüfung

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überwacht als Datenschutzaufsichtsbehörde nach Art. 58 der Datenschutz-Grundverordnung (DS-GVO) die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich im Bundesland Bayern, d. h. in privaten Wirtschaftsunternehmen, bei freiberuflich Tätigen, in Vereinen und Verbänden. Aufgrund der enorm gestiegenen Gefährdungslage im Internet stärkt das BayLDA seinen Fokus auf präventive Maßnahmen zur Cybersicherheit für bayerische Verantwortliche, damit personenbezogene Daten angemessen und wirksam vor den täglichen Gefahren im digitalen Zeitalter geschützt werden. Das BayLDA führt zu diesem Zweck Prüfungen durch, um grundlegende Sicherheitslücken oder Mängel in der IT-Organisation aufzuzeigen und Verantwortliche somit noch vor einem Vorfall hinsichtlich des Bedarfs an durchzuführenden Maßnahmen hinzuweisen. Auch wenn der vorbeugende Charakter der Datenschutzkontrollen des BayLDA hervorgehoben wird, besteht seit der Anwendbarkeit der DS-GVO neben der bereits existierenden gesetzlichen Verpflichtung, für ein ausreichendes Sicherheitsniveau im Umgang mit personenbezogenen Daten zu sorgen, auch grundsätzlich die Möglichkeit, bei (gravierenden) Verstößen gegen die Sicherheit der Verarbeitung nach Art. 32 DS-GVO Geldbußen zu verhängen.

Ransomware – Mehr als „nur" Verschlüsselung von Daten

Die Verschlüsselung von personenbezogenen Daten mittels Schadcode ist ein seit langer Zeit bekannter und gefürchteter Angriff aus der Cybercrime-Welt. Nicht-verfügbare Daten bedeuten für die meisten Unternehmen Produktionsstillstand oder massive Einschränkungen im Arbeitsalltag. Durch die Möglichkeit der faktisch anonymen Bezahlung per Bitcoin können die daraus abgeleiteten Erpressungen zur Wiederentschlüsselung der Daten unmittelbar und meist ohne großes Risiko einer Entdeckung von Cyberkriminellen durchgeführt werden – die strafrechtlichen Ermittlungen gestalten sich aufgrund der Anonymisierungsmöglichkeiten im Internet als schwierig. Datenschutzrechtlich haben solche Sicherheitsvorkommnisse ebenso Konsequenzen: Als Datenschutzverletzung müssen diese der zuständigen Datenschutzaufsicht innerhalb von 72 Stunden nach Kenntniserlangung gemeldet werden. In den vergangenen Jahren wurden dem BayLDA bereits sehr viele Vorkommnisse dieser Art gemeldet, Tendenz steigend.

Verantwortliche begegnen dieser Art der Bedrohung mit zunehmend wirksamen Backup-Konzepten, die einem Angriff mit dem Ziel einer nachhaltigen Datenverschlüsselung unter Umständen standhalten, wenngleich die Wiederherstellung des Datenbestands für viele Betriebe eine Kraftanstrengung im Tagesgeschäft bedeutet. Der größte Aufwand liegt dann darin, Schadcode von den Rechnern zu entfernen, das Einfallstor ausfindig zu machen und zu schließen und letztendlich ein geeignetes Backup einzuspielen. Angreifer-Gruppierungen reagieren jedoch längst auf diese verringerte Wirksamkeit ihrer Schadcode-Kampagnen, indem nach dem erfolgreichen Eindringen in das Netzwerk eines Unternehmens oder nach der Übernahme eines Rechners weiter nach möglichst interessanten Daten, wie Office-Dokumente und Datenbankdateien, gesucht wird. Diese werden nun vor der Verschlüsselung der Daten für die betroffene Organisation unbemerkt auf Server der Angreifer kopiert. Es werden somit gezielt Daten ausgeleitet. Die Erpresser drohen im Falle, dass Lösegeldforderungen nicht beglichen werden, damit, dass

die derart entwendeten Dateien dann entweder im Internet veröffentlicht oder im Darknet an andere Cyberkriminelle verkauft werden. Auch können damit die eigenen Endkunden konfrontiert und erpresst werden.
Eingehende Meldungen zu Verletzungen der Sicherheit nach Art. 33 DS-GVO („Datenschutzverletzungen") beim BayLDA bestätigen, dass dieses Vorgehen weit verbreitet ist. Anhand dieses Trends verändert sich die datenschutzrechtliche Einschätzung von Verschlüsselungstrojanern hinsichtlich der möglichen Schäden grundlegend. Während früher noch häufig von einer ausschließlichen Verschlüsselung ausgegangen wurde und sich das datenschutzrechtliche Risiko nach dem Schaden einer Nicht-Verfügbarkeit von personenbezogenen Daten, IT-Systemen oder Fachprozessen richtete, ist längst auch das Risiko des Vertraulichkeitsverlustes zwingend einzubeziehen. In einer Vielzahl typischer Ransomware-Angriff muss längst davon ausgegangen werden, dass personenbezogene Daten von Angreifern im Kontext von Ransomware entwendet und missbräuchlich weiter verwendet werden. Das Risiko, für die vom Vorfall betroffenen Personen (bzw. für deren Rechte und Freiheiten), dürfte damit als „hoch" einzustufen sein. In der Konsequenz bedeutet dies, dass in solchen Fällen meist auch die betroffenen Personen – z. B. Beschäftigte, Lieferanten, Kunden, Mandaten oder Patienten – gemäß Art. 34 DS-GVO über den Vorfall benachrichtigt werden müssen.

Diese Weiterentwicklung des Ransomware-Vorgehensmodells der Cyberkriminellen bedeutet folglich für Organisationen, die nach einer Ransomware-Infektion nicht von einer Datenausleitung ausgehen, erhöhte Nachweispflichten gegenüber der zuständigen Datenschutzaufsichtsbehörde gerade hinsichtlich der Begründung des Risikos. Insbesondere die Frage einer hinreichenden Wahrscheinlichkeit, dass keine Datenflüsse an die Angreifer stattgefunden haben, muss ausreichend beantwortet werden (z. B. Web-Proxy blockte verdächtigen Serveraufrufe, Datenvolumen im Auswertezeitraum erscheint nicht hoch genug). Nachweise dieser Art sind im Rahmen einer Meldung nach Art. 33 DS-GVO beizulegen.

Weiterführende Links zum Thema:

- ✓ BayLDA: Schadcode Informationsseite
  https://www.lda.bayern.de/de/thema_schadcode.html
- ✓ BSI: Ransomware: Bedrohungslage, Prävention und Detektion 2021
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf
- ✓ BayLDA: Cybersicherheit in medizinischen Einrichtungen
  https://www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf
- ✓ BayLDA: Patch Management Checkliste nach Art. 32 DS-GVO
  https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf
- ✓ BayLDA und BayLfD: Microsoft Exchange Security Check & Incident Response
  https://www.lda.bayern.de/media/themen/exchange_security_check_incident_response.pdf