Bayerisches Landesamt für
Datenschutzaufsicht

Informationsblatt

Absicherung von E-Mail-Accounts zum Schutz vor Phishing und Cyberattacken

Stand: 09.05.2022

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 auf den Bedarf 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 Verantwortliche, für ein ausreichendes Sicherheitsniveau im Umgang mit personenbezogenen Daten zu sorgen, auch grundsätzlich die Möglichkeit für die Datenschutzaufsichtsbehörde, bei Verstößen gegen die Sicherheit der Verarbeitung nach Art. 32 DS-GVO Geldbußen gegen Verantwortliche zu verhängen.

Phishing: Einstiegspunkt für Cyberkriminelle

Durch die Angriffstechnik Phishing sollen potentielle Opfer mittels täuschend echt wirkenden, aber gefälschten E-Mails zu einer bestimmten Handlung animiert werden. Meist werden die Opfer dazu aufgefordert, ebenfalls gefälschte Websites (Fakes-Websites) aufzurufen und Zugangsdaten einzugeben, welche die Betrüger dann abgreifen. Mit diesen können die Angreifer weitere kriminelle Schritte ausführen, wie bspw. das Verbreiten von Schadcode.

Angriffe über E-Mail-Accounts können auch einen enormen unmittelbaren wirtschaftlichen Schaden bedeuten: Cyberkriminelle nutzen durchaus übernommene E-Mail-Accounts, um mit der gestohlenen Identität gezielt finanziellen Betrug zu begehen. So versenden die Angreifer oft E-Mails mit geschäftlichen Informationen, die bei den Mitarbeiterinnen und Mitarbeitern oder auch bei Partnerunternehmen keinen Verdacht eines Betrugs erwecken. Meist werden bei Zahlungen, bspw. für eine Lieferung oder bei einem Vertragsabschluss, die Kontodaten manipuliert, sodass die Buchhaltung den Betrag an die angegebene Bankverbindung überweist. Oftmals fällt ein solcher Betrugsvorgang erst zu spät auf – nämlich dann, wenn die Cyberkriminellen längst mit dem Betrag auf und davon sind.

Datenschutzrechtlich haben derartige Sicherheitsvorkommnisse ebenso Konsequenzen: Sobald es zu einer solchen Sicherheitsverletzung kommt, muss diese bei der zuständigen Datenschutzaufsichtsbehörde innerhalb von 72 Stunden nach Kenntniserlangung gemeldet werden. Das ist in der Regel bspw. bereits dann der Fall, wenn ein einzelner dienstlicher E-Mail-Account von einem Unbefugten übernommen wurde und ein Datenschutzrisiko im

Sinne des Art. 33 DS-GVO entsteht. In den vergangenen Jahren wurden dem BayLDA bereits sehr viele Vorkommnisse dieser Art gemeldet, bei dem der eingetretene Schaden zum Teil enorm war. Betrügerische Finanztransaktionen im sechs- und siebenstelligen Eurobereich sind längst keine Seltenheit mehr. Mit einem Abflachen der Angriffswellen auf E-Mail-Accounts ist daher nicht zu rechnen.

Einfache Abhilfe: Awareness und richtige Administration

Verantwortliche können dieser Art der Bedrohung durch gezielte Kampagnen zum Sicherheits-Bewusstsein begegnen, wobei das eigene Personal umfassend über die Angriffsmöglichkeiten per E-Mail sowie über geeignete Abhilfemaßnahmen unterrichtet werden. Gerade die individuellen Verhaltensweisen der Mitarbeiterinnen und Mitarbeiter im Umgang mit gefälschten E-Mails entscheiden wesentlich darüber, ob es überhaupt zu einem Sicherheitsvorfall kommt. Als Basis wird ein ausreichender Zugangsschutz der E-Mail-Accounts vorausgesetzt, bspw. über starke Passwörter und Mehr-Faktor-Authentifizierungen. Jedoch spielt auch die technische Absicherung der Accounts durch geeignete Administration eine wesentliche Rolle. Das Einspielen von aktuellen Sicherheitsupdates, dem Abfangen von schädlichen E-Mails sowie ein gepflegtes Rollen-/Rechtekonzept sind hierbei besonders wichtig.

Weiterführende Links zum Thema:

- ✓ BSI: E-Mail-Sicherheit
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Buero/E-Mail-Sicherheit/e-mail-sicherheit_node.html
- ✓ BSI: IT-Grundschutz-Kompendium APP.5.2 Microsoft Exchange und Outlook
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/06_APP_Anwendungen/APP_5_2_Microsoft_Exchange_und_Outlook_Edition_2022.pdf?__blob=publicationFile&v=3#download=1
- ✓ BSI: IT-Grundschutz-Kompendium APP.5.3 Allgemeiner E-Mail-Client und -Server
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/06_APP_Anwendungen/APP_5_3_Allgemeiner_E-Mail_Client_und_Server_Edition_2022.pdf?__blob=publicationFile&v=3#download=1
- ✓ BayLDA: Homeoffice Checkliste
  https://www.lda.bayern.de/media/checkliste/baylda_checkliste_homeoffice.pdf
- ✓ BayLDA: Patch Management Checkliste nach Art. 32 DS-GVO
  https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf