Ministerium des Inneren, für Digitalisierung und Kommunen
Baden-Württemberg

17.12.2021

CYBERSICHERHEIT

5 praktische Tipps gegen Hackerangriffe

Gorodenkoff Productions OU

Die Cybersicherheitsagentur Baden-Württemberg schätzt das Risiko eines Cyberangriffs über Weihnachten besonders hoch ein. Erfahrungsgemäß erfolgen gezielte Angriffe häufig über längere Feiertagsphasen wie Weihnachten, Ostern oder Pfingsten.

Weihnachts-Jingles, Nikolaus-Memes oder das besinnliche Kerzen-Bild: Der Weihnachtsgruß im E-Mail-Postfach ist schnell geöffnet. Doch was verbirgt sich wirklich hinter dem Anhang? Die Cybersicherheitsagentur Baden-Württemberg (CSBW) sieht für die Weihnachtsfeiertage ebenso wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein erhöhtes Risiko für Angriffe im Internet und ruft zur Vorsicht auf. Im Fokus der Angriffe stehen vor allem Organisationen, Behörden und Unternehmen, aber auch Privatpersonen können Opfer von Cyberattacken werden. Und die Erfahrung zeigt: Gezielte Angriffe erfolgen häufig über längere Feiertagsphasen wie Weihnachten, Ostern oder Pfingsten. Auch der aktuelle Fall um die Sicherheitslücke Log4Shell in der Java-Bibliothek Log4j, die

derzeit Sicherheitsexperten weltweit beschäftigt und als Einfallstor für zukünftige Angriffe dienen kann, zeigt, dass ein Cyberangriff prinzipiell alle treffen kann.

Kampf gegen Cyberkriminalität zentrale Herausforderung

„Das Jahr 2021 ist nicht nur durch die Pandemie geprägt. Alle Bereiche, Verwaltung, Wirtschaft, Gesellschaft haben einen digitalen Sprung gemacht. Das birgt viele Chancen, freilich auch Risiken, gerade jetzt um den Jahreswechsel. Die aktuellen Warnungen zeigen: Wir müssen vor Cyberkriminellen auf der Hut sein! Der Kampf gegen Cyberkriminalität ist eine der zentralen Herausforderungen unseres Jahrzehnts. Wir alle können einen Teil dazu beitragen, unsere Systeme sicherer zu machen. 5 Tipps haben wir für die Feiertage zusammengestellt!“, sagte Digitalisierungsminister Thomas Strobl.

5 praktische Tipps gegen Hackerangriffe über die Feiertage:

1. **Prüfen Sie alle Ihre Anwendungen** darauf, ob diese von der Sicherheitslücke Log4Shell betroffen sind, bspw. unter folgendem Link. Falls ja, installieren Sie umgehend die von den Herstellern bereitgestellten Updates.
2. Die CSBW rät, **IT-Systeme über die Feiertage und zwischen den Jahren nicht gänzlich unbeaufsichtigt** zu lassen und im Falle eines Cyberangriffs einen Notfallplan parat zu haben. Fachkundige Hilfe für Unternehmen bieten beispielsweise die Zentrale Ansprechstelle Cybercrime beim Landeskriminalamt, die Cyberwehr Baden-Württemberg und in herausgehobenen Fällen sowie für die Behörden des Landes die Cybersicherheitsagentur selbst.
3. Außerdem ist es sinnvoll, wenn Unternehmen ihre **Beschäftigten sensibilisieren** und auf mögliche Gefahren hinzuweisen.
4. Sie haben ein neues Smartphone bekommen, einen neuen Router eingerichtet oder sich mit smarten Einrichtungsgegenständen eine Freude gemacht? **Überprüfen Sie die Sicherheits- und Datenschutzeinstellungen neuer Geräte** und richten Sie Passwörter oder Zugangsdaten umgehend neu ein, belassen Sie nicht die werksseitig bestehenden Passwörter.
5. **Schützen Sie sich vor Phishing-E-Mails!** Grundsätzlich sollte jede E-Mail und jede Messenger-Nachricht gründlich überprüft werden. Die folgende Checkliste der Cybersicherheitsagentur Baden-Württemberg hilft dabei, mögliche Phishing-E-Mails zu erkennen und die Verbreitung von schädlichen Nachrichten zu verhindern. Kontrollieren Sie jede E-Mail auf Grundlage der folgenden Merkmale:

- **Werde ich persönlich angesprochen?** Oftmals wird keine persönliche Anrede genutzt. Ihre Bank und Online-Zahlungsdienste sprechen Sie in E-Mails grundsätzlich mit Ihrem Namen an und niemals mit „Sehr geehrter Kunde“.
- **Wer ist der Absender?** Zumeist ist die Absender-Adresse bei Phishing-E-Mails gefälscht und durch Zusätze wie „Service“ oder „Info“ ergänzt. Achten Sie besonders auf Abweichungen zwischen dem angeblichen Absender und der neben dem Absender stehenden E-Mail-Adresse! Es ist möglich, den Absendernamen einer E-Mail beliebig zu verändern, nicht aber die eigentliche E-Mail-Adresse.
- **Werde ich unter Druck gesetzt?** Betrugs-E-Mails kommunizieren meist dringenden Handlungsbedarf und drohen mit Konsequenzen.
- **Ist der Link oder Anhang vertrauenswürdig?** Betrugs-E-Mails enthalten entweder einen schadhaften Link oder einen schadhaften Anhang. Die Zieladresse des Links können Sie einsehen,

indem Sie mit der Maus über den Link fahren, ohne darauf zu klicken.

- **Fragt der Absender persönliche Daten ab?** Kein seriöser Absender fordert Sie zur Eingabe Ihrer persönlichen Daten per E-Mail oder SMS auf!
- **In welcher Sprache ist die E-Mail verfasst?** Phishing-E-Mails sind manchmal in fremder Sprache verfasst oder wurden fehlerhaft ins Deutsche übersetzt. Es gibt aber auch sehr gut gestaltete und formulierte Phishing-E-Mails, weshalb man sich nicht zu sehr auf dieses Merkmal verlassen sollte.

Angriffe erfolgen täglich und nahezu zu jeder Zeit

Die Zahl der erfolgreichen Angriffe in der Landesverwaltung im Jahr bewegt sich Regel konstant im einstelligen bis unteren zweistelligen Bereich. Hinsichtlich der Verwendung des Begriffes „Cyberattacken" und „Angriffe" sowie der Erhebung ihrer Anzahl ist anzumerken, dass im Bereich der Landesverwaltung solche Angriffe täglich und nahezu zu jeder Zeit festzustellen sind – beispielsweise durch das massenhafte Zuleiten von mit Schadcode versehenen E-Mails oder durch von außen durchgeführte Scans nach Schwachstellen und Sicherheitslücken. Mittels automatisierter, mehrstufiger Schutzmaßnahmen werden alleine in der Landesverwaltung täglich über eine Million an Spam-E-Mails und virenbehafteten E-Mails ausgefiltert. Ebenso wird an den Firewalls und Schutzsystemen täglich eine hohe Zahl – teilweise mehrere hundert – automatisiert durchgeführte Scans nach Schwachstellen und Sicherheitslücken detektiert und geblockt. Insbesondere diese sind begrifflich als Angriff / Cyberattacke zu werten. Insgesamt ist die Tendenz der erfolgten Angriffe und Angriffsversuche nach wie vor konstant steigend.

Die Cybersicherheitsagentur sensibilisiert zu all diesen Themen, sodass Sicherheitsvorfälle möglichst gar nicht erst auftreten. Für Beschäftigte der Landesverwaltung und der Kommunen startet die CSBW eine Sensibilisierungskampagne für 2022, in der mit vielen Tipps und Hilfestellungen die Cybersicherheit gestärkt werden soll.

Ergänzende Information zu Cyberattacken

Als Haupteinfallstor für Cyberattacken zählen sogenannte Phishing-E-Mails. Sie können extrem hohe wirtschaftliche und betriebliche Schäden verursachen. Cyberkriminelle versuchen dabei, über gefälschte Nachrichten, in denen sie auf gefälschte Webseiten verlinken, an vertrauliche Informationen wie Passwörter, Zugangsdaten oder Kreditkartennummern zu gelangen. Immer öfter enthalten diese E-Mails aber auch Malware-behaftete Datei-Anhänge, die Schadsoftwares wie Trojaner oder Ransomware auf diesem Weg einschleusen sollen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht von einer deutlichen Zunahme der Fallzahlen bei Angriffen mit Ransomware für das Jahr 2021 aus. Es warnt insbesondere auch vor der zunehmenden Bedrohung durch Emotet – ein Schadprogramm, das durch Spam-Kampagnen verteilt wird und sich durch authentisch wirkende E-Mails Zugang verschaffen möchte. Besonders gefährlich an Emotet ist, dass es als „Türöffner" für weitere Malware dient. Ist die Schadsoftware einmal auf dem Computer des Betroffenen installiert, können Cyberkriminelle weitere Schadprogramme nachladen.

Eine Umfrage des Digitalverbands Bitkom zeigt, dass immer mehr Menschen Opfer von Cyberkriminalität werden. Acht von zehn Personen (79 Prozent) geben inzwischen an, dass sie in den

vergangenen 12 Monaten Angriffe im Netz erlebt haben. Fast die Hälfte der Befragten (47 Prozent) hat bereits Erfahrungen mit Schadprogrammen gemacht.

Die Cybersicherheitsagentur Baden-Württemberg

Die Cybersicherheitsagentur ist zentrale Koordinierungs- und Meldestelle im Bereich Cybersicherheit in Baden-Württemberg. Sie sammelt ständig Daten zu Sicherheitslücken, Schadprogrammen und erfolgten oder versuchten Angriffen auf die Cybersicherheit. Hierfür nimmt sie auch direkt Meldungen von Betroffenen entgegen. Alles Relevante dokumentiert sie und wertet die Daten aus. Anhand der Erkenntnisse erstellen die Expertinnen und Experten der CSBW ein immer aktuelles, landesweites Lagebild. Über dieses Lagebild informiert die CSBW beispielsweise andere Behörden. Außerdem warnt sie bei besonderen Gefahren explizit. Zudem vernetzt die CSBW Staat, Verwaltungen, Kommunen, Wirtschaft, Wissenschaft und Forschung im Bereich der Cybersicherheit.

Für Behörden des Landes und an das Landesverwaltungsnetz angeschlossene Organisationen kann die CSBW auch Anordnungen treffen und Maßnahmen zu deren Schutz ergreifen.

Bei Cyberangriffen oder anderen Vorfällen kann die CSBW Landesbehörden, Städten und Gemeinden helfen, auch bei der Wiederherstellung der Systeme nach einem Angriff. In Einzelfällen können auch andere Organisationen mit wichtiger Bedeutung für das öffentliche Gemeinwesen Hilfe erhalten. Bürgerinnen und Bürger sowie Personen in den Bereichen Wirtschaft, Wissenschaft und Verwaltung werden von der CSBW zum Thema Cybersicherheit sensibilisiert. Polizeiliche Aufgaben wie die Strafverfolgung nimmt die CSBW nicht wahr. Sie arbeitet aber eng mit dem Landeskriminalamt, dem Landesamt für Verfassungsschutz sowie anderen Sicherheitsbehörden zusammen.

Über die Landesgrenzen hinaus ist die CSBW zentrale Ansprechpartnerin für Organisationen der Cybersicherheit in Deutschland, sowohl auf Bundes- wie auch Länderebene (wie z. B. das Hessen Cyber Competence Center H3C und das bayrische Landesamt für Sicherheit in der Informationstechnik), in der Europäischen Union (EU) sowie international.