Bayerisches Landesamt für Datenschutzaufsicht

Auftragsverarbeitung im Fokus von Cyberkriminellen

Wie sicher ist Ihre Lieferkette?

Dorit Buschmann
Referentin im BayLDA
Bereich „Cybersicherheit und technischer Datenschutz“

Wer steht heute vor Ihnen?

Dorit Buschmann

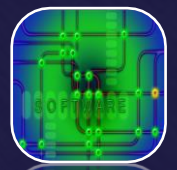
Referentin beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

Bereich „Cybersicherheit und Technischer Datenschutz“

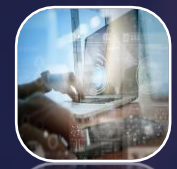
Cybersicherheit

Cyberabwehr Bayern

Ransomware



Enforcement



Zusammenarbeit national/ international

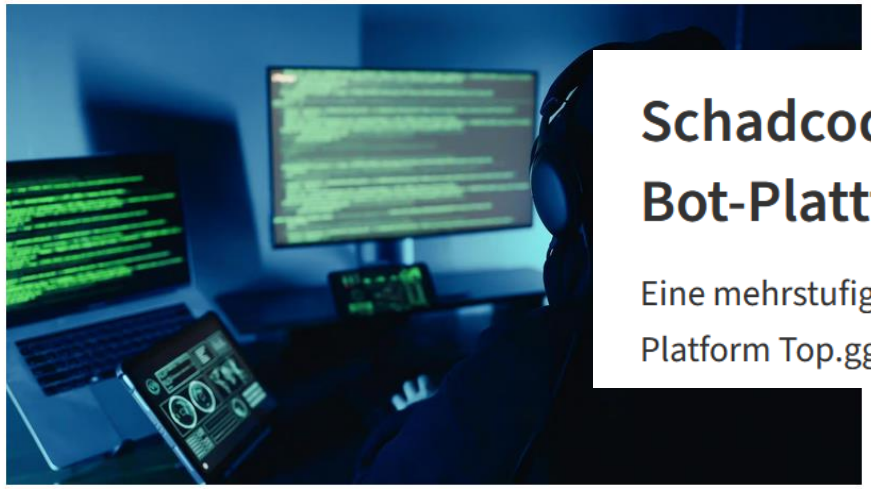
Was ist das für eine Behörde?

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

- Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich in Bayern
- Aufgabe: Sicherstellung, dass sich alle bayerischen Unternehmen, Vereine, Rechtsanwälte, Ärzte, … an die DS-GVO halten
- Sitz in Ansbach
- Zuständig für ca. 800.000 datenschutzrechtlich Verantwortliche
- Ist auch Bußgeldstelle nach DS-GVO

Was ist ein Supply-Chain-Angriff?

Handwerkskammern gehackt: Die kruden Methoden der Cyber-Kriminellen



Schadcode in Python-Paketen trifft Discord-Bot-Plattform mit 170.000 Usern

Eine mehrstufige Supply-Chain-Attacke hat unter anderem erfolgreich die Platform Top.gg infiltriert und Schadcode an die User verteilt.

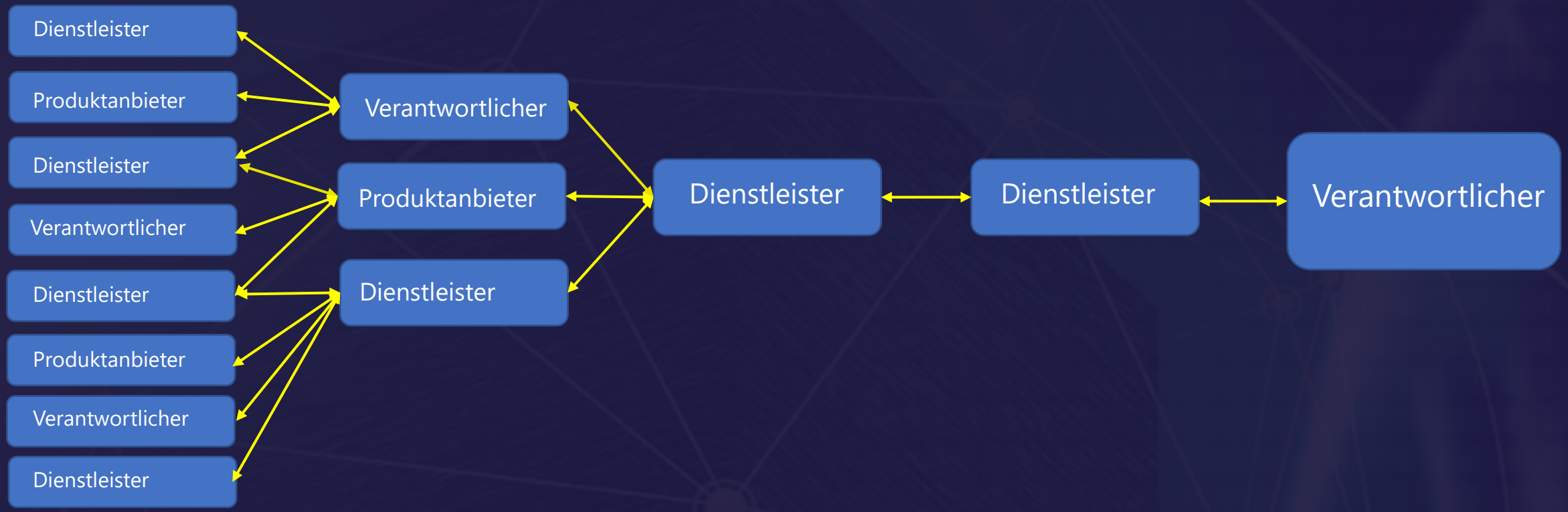
Drittanbieter-Sicherheitslücke

Hacker prahlen mit Amazon-Leak auf BreachForums

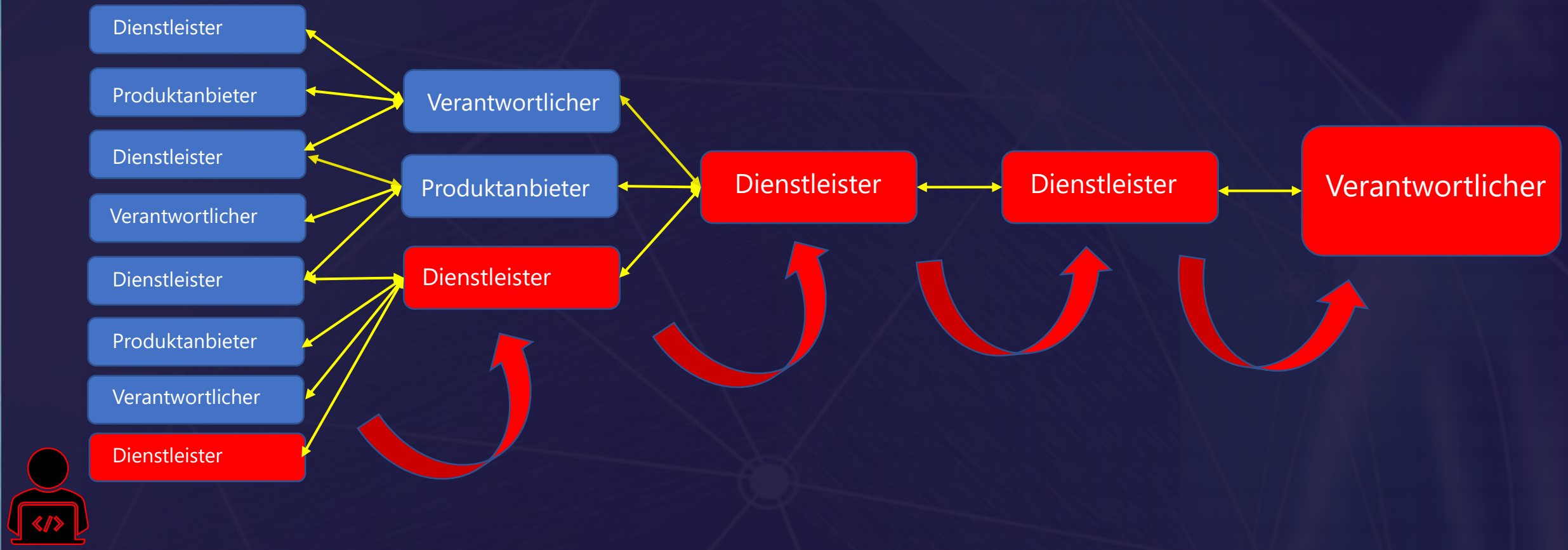
12. November, 2024 09:22

Bildquelle: MacroEcon /Shutterstock.com

Was ist ein Supply-Chain-Angriff?



Was ist ein Supply-Chain-Angriff?



Was ist ein Supply-Chain-Angriff?

- Aktuell Angriffe mit sehr großen Auswirkungen – z. B. MOVEit (ca. 2800 betroffene Organisationen mit bis zu 96 Millionen betroffenen Personen)
- Supply-Chain-Angriffe gibt es an sich schon viele Jahre
- Aber: Angriffe auf Lieferketten nehmen immer mehr zu

Quelle: Enisa (2021)

Was ist ein Supply-Chain-Angriff?

- Lieferketten sind sehr umfangreich und komplex
- Oft Zusammenarbeit mit vielen Dienstleistern, die wiederum vielfältige Produkte einsetzen

Daraus ergeben sich folgende Probleme:

- Unternehmen verlassen sich auf die Sicherheit der Drittanbieter – das macht Angriffe auf Drittanbieter so erfolgreich
- Zugriff auf (personenbezogene) Daten auch weit entfernt vom „Tagesgeschäft“ vor-Ort, staatliche Zugriffe sind meist gar nicht festzustellen

Zusammenspiel mit Auftragsverarbeiter

- DS-GVO adressiert Verantwortliche und Auftragsverarbeiter – letzte Verantwortlichkeit bleibt aber beim Auftraggeber
- Verantwortlicher muss sicherstellen, dass bei allen Auftragsverarbeitern und allen eingesetzten Produkten die Anforderungen aus der DS-GVO erfüllt sind
- Konsequenz: Nur Auftragsverarbeiter, die das gleiche, angemessene Schutzniveau wie beim Verantwortlichen erreichen, dürfen laut DS-GVO eingesetzt werden – ebenso auch nur Einsatz von Produkten, die dem nicht entgegenstehen

Zusammenspiel mit Auftragsverarbeiter

- Art. 28 Abs. 1 DS-GVO und Art. 32 DS-GVO müssen beachtet werden
- TOM auch bei Auftragsverarbeitung
- Datenübertragung somit nur an Empfänger, die selbst TOM (nach DS-GVO) einhalten

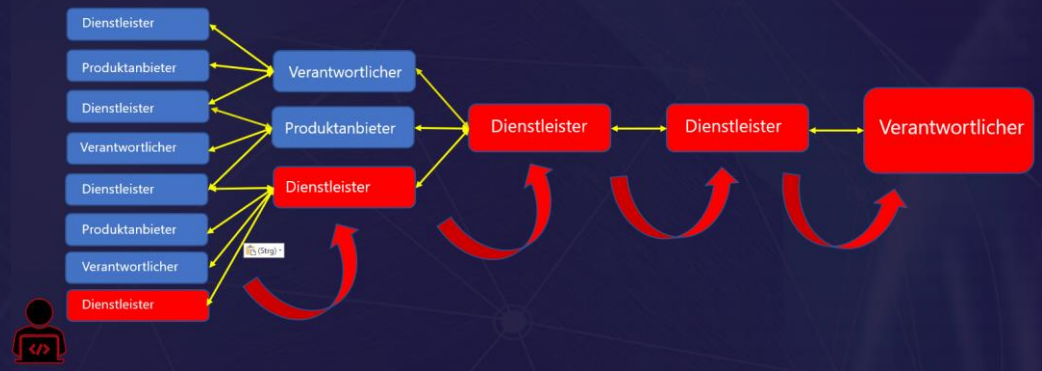
Art. 28 DSGVO

Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Meldepflichten bei Sicherheitsverletzungen

- Die Risikobeurteilung und ggf. Meldungen an Aufsichtsbehörden/Betroffene trifft der Verantwortliche
- Meldeverpflichtung über gesamte Supply-Chain durchgehend vom Auftragsverarbeiter in Richtung Verantwortlicher
- Betrifft auch Sub-Auftragsverarbeiter
- Bei Auslöser in Produkten (z. B. Log4Shell-Lücke) muss der Verantwortliche selbst auf das Vorhandensein einer Handlungserfordernis prüfen
- Auftragsverarbeiter können aber Bußgeldadressaten sein



Wie passt das alles zusammen?

- Bei der Weitergabe personenbezogener Daten an Auftragsverarbeiter muss ein angemessenes Schutzniveau sichergestellt werden – gilt auch für Unterauftragsverarbeiter und beim Drittlandtransfer
- EU-Standardvertragsklauseln sehen ebenfalls ein hohes Schutzniveau vor
- Transfer Impact Assessments schaffen bezüglich Behördenzugriffe Klarheit und leiten ggf. restriktivere Schutzmaßnahmen ein
- Im Worst-Case: Umsetzung von Supplementary Measures mit den Folgen extrem eingeschränkter Verarbeitungsmöglichkeiten
- Aber: Der Umgang mit Supply-Chain-Angriffe als „Angriffstrend" ist durch die Instrumente der DS-GVO schon gut abgedeckt

Checkliste Supply-Chain-Angriffe

- ✓ Verzeichnis der Verarbeitungstätigkeiten ist vollständig und aktuell
- ✓ Liste aller Auftragsverarbeiter und Unterauftragsverarbeiter ist vollständig und aktuell
- ✓ Auftragsverarbeiter werden auch danach ausgewählt, dass diese als „verlässliche Partner“ bei der Einhaltung der DS-GVO angesehen werden (Art. 28 Abs.1 DS-GVO)
- ✓ Schutzniveau der Auftragsverarbeiter wird anhand einer Dokumentenprüfung bestimmt. Diese umfasst auch den Einsatz von Produkten beim Auftragsverarbeiter
- ✓ Meldungen von Sicherheitsverletzungen durch (Unterauftrags-)Verarbeiter funktionieren. Informationen über bekannte gravierende Schwachstellen werden bereitgestellt

Checkliste Supply-Chain-Angriffe

- ✓ Technische und organisatorische Schutzmaßnahmen der EU-Standardvertragsklauseln sind bekannt und werden bei der Auswahl der (Unterauftrags-)Verarbeiter berücksichtigt
- ✓ Beim Transfer in die USA auf Grundlage des EU-US-Datenschutzrahmens: Es werden nur allgemeine Schutzmaßnahmen bzw. Garantien insbesondere gegen Cyberkriminelle geprüft (und auch ob Meldungen über Sicherheitsverletzungen funktionieren)
- ✓ Beim Transfer in unsichere Drittländer werden behördliche Zugriffsrisiken in die Bewertung aufgenommen – Prüfung über EU-Standardvertragsklauseln samt Transfer Impact Assessments
- ✓ Supplementary Measures werden als letztes Mittel eingesetzt. Es ist bekannt, dass viele Verarbeitungen dann nicht mehr gehen

Supply-Chain-Angriffe - Fazit

- Rechtsinstrumente der DS-GVO zur Sicherstellung eines ausreichenden Schutzniveaus entlang der Supply-Chain sind bereits vorhanden
- Regelungen zum Drittlandtransfer sind wirksam (und mit Blick auf Supplementary Measures auch restriktiv)
- Auswahl geeigneter Dienstleister aus Datenschutzperspektive bleibt eine Herausforderung
- Unterauftragsverarbeiter dürften (Stand heute) wohl vielen Verantwortlichen noch nicht vollständig bekannt sein
- Sicherheitsmaßnahmen bei Auftragsverarbeitung sind heute i. d. R. kein Problem mehr. Tipp: Den Dienstleister verpflichten ein der DS-GVO entsprechendes Schutzniveau dauerhaft zu etablieren
- Meldeketten bei Sicherheitsverletzungen dürften umso schlechter funktionieren, je weiter ein Dienstleister in der Supply-Chain vom Verantwortlichen „weg“ ist sowie umso schwächer der aufsichtliche Vollzug ist

Vielen Dank für Ihre Aufmerksamkeit.

Cyberprävention
Mehr Sicherheit durch Datenschutz
www.lda.bayern.de