tulmera
Ihr Partner für IT Beratung

Sicherheitsvorfall bestätigt? Was nun?

Spasimira Goncheva-Kompa
Gründerin von
Tulmera GmbH

Agenda

- Vorstellung Tulmera GmbH
- Warum sind wir alle potenzielle Ziele?
- Angriffsprävention vs. Reaktionsmechanismen
(inkl. Incident Responce Plan und Best Practies)
- Meldepflichten und Fristen
- Zusammenfassung und Handlungsempfehlungen

Tulmera GmbH

Nach 19 Jahren Erfahrung in der IT – sowohl als Beraterin als auch als interne Mitarbeiterin – habe ich mich dazu entschieden, mein eigenes Unternehmen zu gründen. Dieser Schritt war für mich die logische Konsequenz aus dem Wunsch, meine umfassende Bildung, mein Wissen und meine langjährige Erfahrung uneingeschränkt einzubringen.

Was als „One-Woman-Show“ begann, hat sich inzwischen zu einem engagierten Team entwickelt. Gemeinsam setzen wir auf kurze Entscheidungswege und gestalten unsere Arbeit flexibel, effizient und zielgerichtet. Unsere Unabhängigkeit gibt uns die Freiheit, ohne äußere Einschränkungen zu agieren und unser volles Potenzial auszuschöpfen.

Diese Entwicklung ermöglicht es uns, unsere Expertise eigenständig und authentisch einzusetzen. Wir arbeiten in einem Umfeld, das nicht nur unsere beruflichen, sondern auch unsere persönlichen Werte widerspiegelt und unsere Leidenschaft für nachhaltige, lösungsorientierte IT-Arbeit fördert.

Mehr zu uns unter https://www.tulmera.com/unser-team/

Warum sind wir alle potenzielle Ziele?

01

Cyberangriffe betreffen nicht nur Unternehmen, sondern auch Einzelpersonen.

02

Phishing, Social Engineering, Ransomware und Identitätsdiebstahl sind weit verbreitet.

03

Daten sind wertvoller denn je – für Unternehmen und Kriminelle.

04

Mit Technologie und KI-Algorithmen werden Angriffe raffinierter.

05

Sicherheit erfordert proaktive Maßnahmen und Reaktionspläne.

Warum sind wir alle potenzielle Ziele? Technologische Entwicklung und KI

Zunehmende Automatisierung

Moderne Angriffe nutzen KI, um Phishing-E-Mails zu perfektionieren oder Sicherheitslücken automatisiert auszunutzen. Dadurch werden Cyberangriffe effizienter und schwerer zu erkennen.

Deepfake- und Social- Engineering- Angriffe

Fortschrittliche KI-Modelle ermöglichen täuschend echte Deepfake-Anrufe oder Videos, mit denen Hacker Vertrauen erschleichen und Zugang zu sensiblen Informationen erhalten.

Herausvorderung für Sicherheitsteams

Während KI von Angreifern genutzt wird, müssen Sicherheitsabteilungen ebenfalls auf KI-gestützte Abwehrmechanismen setzen, um mit der rasanten Entwicklung Schritt zu halten.

Angriffsprävention vs. Reaktionsmechanismen

01

Präventive Maßnahmen, wie Frameworks für Cybersicherheit, Zertifizierungen für Fachkräfte reduzieren das Risiko von Sicherheitsvorfällen.

02

Firewalls, Penetrationstests und Sicherheits-Audits, Patch- und Schwachstellenmanagement, Regelmäßige Backups und Tests, MFA und regelmäßige Awareness Schulungen sind essenziell.

03

Reaktionsmechanismen helfen, Angriffe schnell zu erkennen und einzudämmen.

04

Ein gut definierter Incident-Response-Plan ist entscheidend.

05

Dokumentation und Nachbereitung verbessern zukünftige Sicherheitsstrategien.

Angriffsprävention vs. Reaktionsmechanismen Forensik und Nachverfolgung

Warum Spurenanalyse entscheidend ist

Jeder Angriff hinterlässt digitale Spuren, die es ermöglichen, Täter zu identifizieren und zukünftige Attacken zu verhindern.

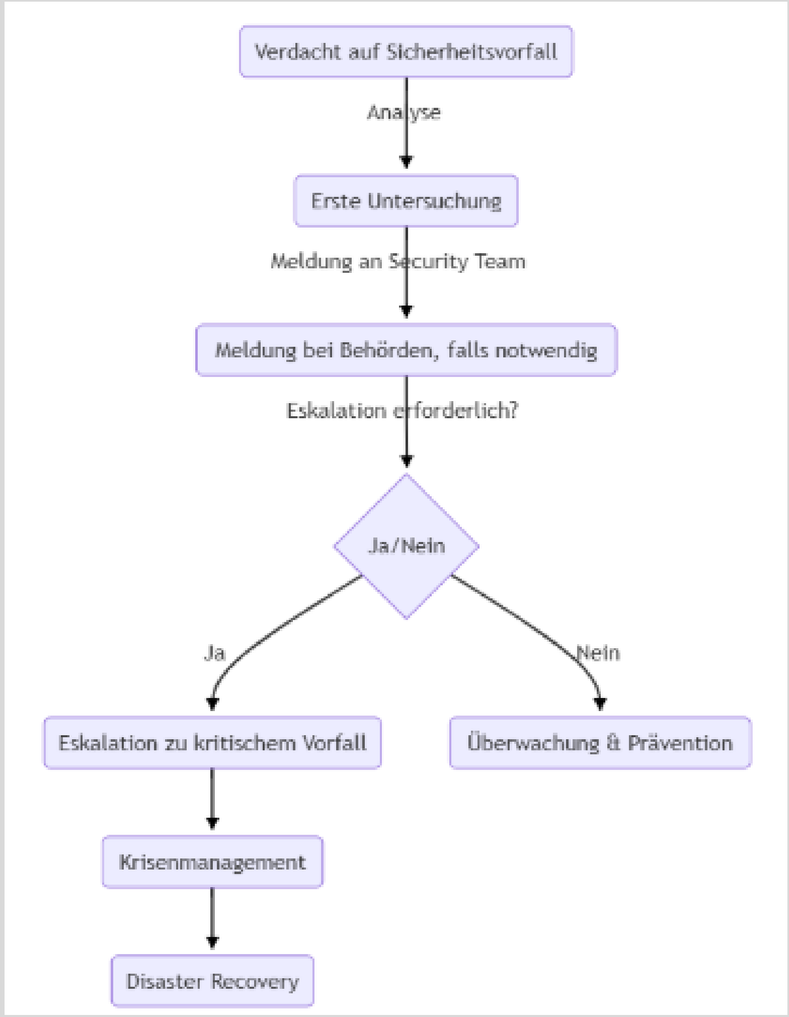
Wichtige forensische Techniken

Log-Analysen, Speicherforensik und Netzwerkverkehrsanalyse helfen dabei, Sicherheitsvorfälle aufzuklären.

Kooperation mit Behörden

Behörden wie das BSI oder das CERT unterstützen bei der Untersuchung und Dokumentation von Angriffen.

Sicherheitsvorfall Prozessablauf



Erste Maßnahmen nach einem Sicherheitsvorfall

!Zuerst: Ruhe bewahren!

01

Sofortmaßnahmen zur Schadensbegrenzung ergreifen (z.B. den betroffenen Bereich isolieren

02

Erste Schadensanalyse durchführen

03

Vorfall dokumentieren und interne Eskalation starten. Sicherstellung von Beweisen und Forensik

04

Abstimmung mit IT-Sicherheit und Datenschutz (Incident Responce Team)

05

Bewertung der Meldepflichten und Zuständigkeiten

Best Practices

01

Sicherheitsprozesse müssen **regelmäßig aktualisiert** werden.

02

Eskalationspläne müssen klar definiert und getestet werden.

03

Technische und **organisatorische** Maßnahmen müssen **zusammenwirken**.

04

Schulungen für Mitarbeiter erhöhen das Sicherheitsbewusstsein.

05

Transparenz und **Kommunikation** sind entscheidend für eine effektive Sicherheitsstrategie.

Meldepflichten und Fristen

Meldepflicht bei Datenschutzverletzungen

Nach Artikel 33 DSGVO muss eine Datenschutzverletzung innerhalb von 72 Stunden an die zuständige Datenschutzbehörde gemeldet werden, sofern ein Risiko für betroffene Personen besteht.

Meldepflichten nach IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz und NIS2 erfordern von Betreiber kritischer Infrastrukturen eine schnelle und transparente Meldung kritischer Vorfälle. Die Meldung erfolgt an das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Auswirkungen von verspäteten Meldungen

Bei verspäteter/unterlassener Meldung drohen hohe Strafen (Bußgelder von bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes) und Vertrauensverlust bei Kunden und Partnern.

Zusammenfassung und Handlungsempfehlungen

Was können Unternehmen und Einzelpersonen tun, um sich besser zu schützen?
Sicherheitsvorfälle lassen sich nicht zu 100 % vermeiden, aber durch präventive Maßnahmen, schnelle Reaktionen und klare Prozesse können Risiken minimiert und Schäden begrenzt werden.

Welche Maßnahmen müssen Unternehmen und Einzelpersonen nach einem Sicherheitsvorfall dringend ergreifen?
Erstmal Ruhe bewahren! Dann schnell und effizient reagieren: Vorfall dokumentieren, Sofortmaßnahmen einleiten, Behörden informieren und Betroffene schützen. Die Einhaltung der Meldepflichten ist entscheidend, um rechtliche Konsequenzen zu vermeiden.

tulmera
Ihr Partner für IT Beratung

Danke für Eure Aufmerksamkeit!

Spasimira Goncheva-Kompa
info@tulmera.com
www.linkedin.com/company/tulmera-gmbh