„Datensicherheit-Cyberkriminalität, die unsichtbare Gefahr“

Vortrag beim 12.Tag der saarländischen Versicherungswirtschaft

Ihr Dozent

Rechtsanwalt Jörg Conrad

Mitarbeiter der Firma GINDAT GmbH

Vorstellung GINDAT GmbH

GINDAT GmbH

Gesellschaft für **I**T-**N**ormierung und **Dat**enschutz

Geschäftsführer:

- Arndt Halbach, TÜV-zertifizierter Datenschutz-Auditor
- Dr. Hans Daldrop, zertifizierter Datenschutzbeauftragter

Vorstellung GINDAT GmbH

Mitarbeiter: Zurzeit acht Festangestellte im Backoffice, davon vier Juristen

Kunden: Weltweit, davon ca. 500 im Datenschutz aus unterschiedlichen Branchen. Ein besonderer Schwerpunkt ist der Versicherungsvermittler

Vorstellung GINDAT GmbH

Was die GINDAT leisten kann:

- Bereitstellung eines externen Datenschutzbeauftragten (DSB)
- Beratung im Datenschutz und Aufbau eines Datenschutzmanagements
- Schulung von Mitarbeitern
- Individuelle Datenschutz-Pakete für Unternehmen
- Unterstützung zur Verbesserung der IT-Sicherheit
- Vorbereitung, Durchführung von Sicherheits- u. Netzwerkaudits
- Vorbereitung von Sicherheitsmaßnahmen auf Grundlage der ISO / IEC 27001
- Implementierung des Datenschutzes im Qualitätsmanagement

Die Datenschutzgrundverordnung

Ab dem 25.05.2018 gilt die EU-Datenschutzgrundverordnung (DSGVO) und regelt den Umgang mit personenbezogenen Daten.

Darüber hinaus gibt es seit dem 25.05.2018 ein Bundesdatenschutzgesetz neuer Fassung (BDSG).

Die Datenschutzgrundverordnung

Zentraler Begriff für die Anwendung der Verordnung ist die Verarbeitung von personenbezogenen Daten(Art.4 Nr.2)

Die Verarbeitung umfasst sämtliche Vorgänge, wie Erheben, Erfassen, die Organisation, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

=> Auch die Datenverarbeitung in Akten fällt unter die DSGVO

Grundsätze der (Daten-)Verarbeitung (Art.5)

- Rechtmäßigkeit	Auf rechtmäßige Weise (Treu- und Glauben)
- Transparenz	Nachvollziehbarkeit, Informationspflichten
- Zweckbindung	Zwecke sollen vor der Verarbeitung feststehen
- Datenminimierung	Nur die für den Zweck notwendigen (erforderliche) Daten dürfen verarbeitet werden
- Richtigkeit	unrichtige Daten müssen berichtigt werden
- Speicherbegrenzung	Speicherung von Daten nur solange erforderlich
- Integrität/Vertraulichkeit	Schutz vor unbefugter Verarbeitung, Verlust, Zerstörung durch techn./organis. Maßnahmen
- Rechenschaftspflicht	Die Grundsätze sind nachzuweisen

Datenschutzgrundverordnung

Meldepflichten bei Datenschutzverletzungen, Artikel 33

- Eine Verletzung des Schutzes von personenbezogenen Daten meldet dies der Verantwortliche der Aufsichtsbehörde, es sei denn, dass die Verletzung nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Bei einem hohen Risiko für die Rechte und Freiheiten von Betroffenen ist auch der Betroffene zu informieren.

  - Verlust eines Laptops
  - Verlust von Daten durch Angriff auf die IT
  - Versehentliches Öffnen eines Links in einer E-Mail
  - Versehentliches Übersenden einer E-Mail an einen Anderen Empfänger

- Meldung, spätestens binnen 72 Stunden gegenüber der Aufsichtsbehörde
- Umfangreiche formale Vorgaben für die Meldung

Sanktionen

Verhängung von Geldbußen durch die Aufsichtsbehörden, Art. 83

- Geldbußen für Verstöße gegen bestimmte Bestimmungen der DSGVO von bis zu 10.000.000 € oder 2 % des weltweiten Jahresumsatzes
- Geldbußen für Verstöße gegen bestimmte Bestimmungen der DSGVO von bis zu 20.000.000 € oder 4 % des weltweiten Jahresumsatzes
- Bei Nichtbefolgung von Anweisungen(Art. 58 Abs.2) drohen Geldbußen bis zu 20.000.000 €
  oder 4 % des weltweiten Jahresumsatzes

Die Aufsichtsbehörden sind derzeit noch zurückhaltend, bis jetzt wurden 75 Bußgelder verhängt (davon im Saarland lediglich 3) mit einer Gesamtsumme von 449.000 € - Quelle: heise.de v. 14.05.2019.
Die Behörden haben aber bereits angekündigt, dass „die Schonzeit“ vorbei ist.

Datensicherheit

Sicherheit der Datenverarbeitung, Artikel 32

Jeder Verantwortliche trifft geeignete technische und organisatorische Maßnahmen (TOM) um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Schutzziele sind

Es ist die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit (neu) der Systeme und Dienste der Verarbeitung personenbezogener Daten sicherzustellen.

Zu berücksichtigen ist

- Die Verfügbarkeit von personenbezogenen Daten soll bei einem Zwischenfall rasch wiederhergestellt werden können
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM soll etabliert werden.

Datensicherheit
durch geeignete technische Maßnahmen (TOMs)

Sichere Passworte
Verschlüsselung von mobilen Geräten
Verschlossene Büros und Schränke
Regelmäßige Backups und Updates
Sensibilisierung der Mitarbeiter
Videoüberwachung
Prüfung durch Externe

Schredder oder Datentonnen nutzen
Sensibilisierung der Mitarbeiter
Aktueller Virenschutz, Firewall,
Server besonders gesichert
Alarmanlage
USV
Sichere Auswahl von Dienstleistern

Gt(z#X“9t

Cyberkriminalität

Schäden durch Spionage, Sabotage und Datendiebstahl

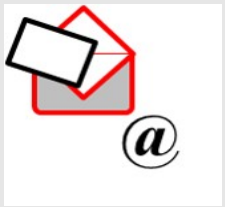
Deutschland bleibt als Wirtschaftsstandort ein bevorzugtes Ziel von Hackern und Computerbetrug. Fast 86 000 Fälle von Cyberkriminalität wurden 2017 von der Polizei bundesweit erfasst Die dadurch entstandenen Schäden lagen bei 71,4 Millionen Euro.

(Quelle BKA-Bundeskriminalamt)

Wie hoch ist das tatsächliche Ausmaß von Cyberkriminalität?

Lediglich neun Prozent der Straftaten werden nach Einschätzung der Sicherheitsexperten zur Anzeige gebracht, die Dunkelziffer liegt damit bei rund 90 Prozent. Deutlich höher sind daher die der Industrie verursachten Schäden. Der IT-Branchenverband Bitkom spricht von 55 Milliarden Euro.

Cybercrime und Angriffe



Pishing Mails

Der Empfänger (das potentielle Opfer) erhält eine E-Mail vom angeblichen Telefonanbieter, Mailprovider, Onlineshop, Kreditunternehmen, Bewerbern usw. mit der Aufforderung

- zum Aufrufen einer Webseite (gefälschte/mit Schadsoftware befallene Internetseite) oder
- zum Öffnen eines Anhanges (z.B. Vertragsdetails, Rechnung, Inkassoschreiben, Widerruf)
- zum Installieren von Software (aus Mail oder Webseite) oder
- zum Antworten per Mail

Cybercrime und Angriffe

Häufigste Folge bei Öffnen von Anhängen oder Links ist die sogen. Ransomeware. Stichwort : („Lösegeld“).

€ € € € €

Eine Ransomware-Welle führt derzeit vielfach zu erfolgreichen Infektionen von Arbeitsplatzrechnern und Netzwerken, bei denen Dateiordner und Dateien in großem Umfang verschlüsselt werden und Lösegeld erpresst wird.

(Quelle BSI aus November 2018)

Bekannte Beispiele von Verschlüsselungstrojanern sind WannaCry, CryptoLocker, GrandCrab oder Locky

Cybercrime und Angriffe

Was ist zu tun?

- Verwenden Sie eine Antivirensoftware, die ein und ausgehende E-Mails überprüft
- Öffnen Sie keine E-Mailanhänge von unbekannten Absendern
- Öffnen Sie keine E-Mailanhänge von Bekannten/bekannten Firmen, ohne dies zu hinterfragen
- Folgen Sie keinen Links, die Ihnen per E-Mail zugeschickt werden („klicken Sie hier um Ihr Bankkonto zu verifizieren“
- Informieren Sie sich über aktuelle Bedrohungen z.B. über die Seite des Bundesamt für Sicherheit in der Informationstechnik (bsi.bund.de)

Sensibilisieren Sie Ihre Mitarbeiter, der Faktor Mensch spielt eine entscheidende Rolle

Cybercrime und Angriffe

Was ist zu tun?

Wichtig ist ein sicheres Backup-Konzept und die Möglichkeit der kurzfristigen Widerherstellung Ihrer Daten

- Sicherung über
- Externer Festplatten
- Bänder
- NAS
- Spiegelung von Festplatten
- Cloud Lösung

Wichtig: Datensicherung sollte an einem externen Standort aufbewahrt werden. Auch Backups können, wenn nicht Offline Ziel von Angriffen werden.

Cybercrime und Angriffe

Social Engineering - CEO-Fraud

- Die Täter sammeln Informationen über entscheidungsrelevante Personen in der Regel die Geschäftsführer (CEO für Chief Executive Officer) sowie deren Sekretariate/Mitarbeiter.
- Im Anschluss werden Personen, die sehr wahrscheinlich auch über die Kontogewalt verfügen per Mail angeschrieben. Der Empfänger soll die Mail absolut vertraulich behandeln, da es z.B. um eine geheime Firmenübernahme oder geheimem Großauftrag geht, wofür unbedingt ein hoher Geldbetrag überwiesen werden muss.
- Da die Mail optisch gefühlt vom "Chef" kommt, wird ziemlich schnell den Anweisungen Folge geleistet und das Geld überwiesen.

Cybercrime und Angriffe

Social Engineering

Umleitung von Zahlungsströmen:

Cyberkriminelle geben – nachdem sie sich in die Server gehackt haben – als Geschäftspartner oder Lieferant eines Unternehmens aus. Mit einem gefälschten Schreiben teilen sie dem Unternehmen mit, dass sich die bisher vereinbarte Bankverbindung geändert hat und der Zahlungsverkehr nun über die neue Bankverbindung erfolgen soll.

Cyber Versicherungen

Weitere Maßnahme: Abschluss eine Cyber-Versicherung?

Im Kern tritt die Cyber-Versicherung ein für Schäden des Versicherten (Eigenschaden) oder Dritter (Drittschaden) durch ungewollte Einwirkungen, Zugriffe und Nutzung von IT-Systemen des Versicherten.

Näheres hierzu erfahren Sie in einem weiteren Vortrag

Zum Schluss

Danke für Ihre Aufmerksamkeit !
Noch Fragen?

GINDAT GmbH
Wetterauer Str. 6
42897 Remscheid
Tel. (0 21 91) 909-430
E-Mail: datenschutz@gindat.de