HINGESCHAUT
Datenschutz im Blick

Sehr geehrte Geschäftsführungen,
liebe Mandanten,

KW 43/2023

es ist wieder so weit. Wieder einmal weitere Informationen rund um die Themen Datenschutz und Datensicherheit.
Auch, wenn Sie vermutlich regelmäßig mit einer Vielzahl von diversen Informationen förmlich zugeschüttet werden, so möchte ich Ihnen dennoch ans Herz legen auch diesmal wieder ein wenig zu schmökern.
Durch die Digitalisierung, die unser Leben immer mehr bestimmt, ist die Beachtung von Datenschutz und Datensicherheit sowohl für Unternehmen als auch für Privatpersonen eine absolute Notwendigkeit.

Viel Spaß beim Lesen wünscht Ihnen das Team der DatCon GmbH.

IT-Security-Fehler von Mitarbeiterinnen und Mitarbeitern

Ja, es war, es ist und es bleibt das schwächste Glied in der Kette. Der Mensch!
Die technischen Schutzmaßnahmen können noch so gut sein, wenn der Mensch zu neugierig ist oder nicht weiß, wie er sich verhalten soll. Wo können nun die Unternehmen ein Stück mehr darauf achten? Denn, ein Sicherheitsvorfall ist in vielen Fällen auch eine Datenpanne gem. DSGVO.

1. Zu schwache Passwörter
   Menschen machen es sich oft einfach und verwenden einfache, leicht zu erratende Passwörter. Zumindest versuchen sie es oftmals. Auch versucht man das gleiche Passwort für mehrere Dienste zu nutzen, was Cyberrisken erhöht. Oder es werden nur leicht veränderte Passwörter genutzt.
   Maßnahmen? Hier helfen technische und organisatorische Richtlinien zur sicheren Passwortvergabe. Es muss eine Vorgabe gemacht werden, eine Richtlinie gegeben werden.
2. Unvorsichtiger E-Mail-Gebrauch
   Nichts Neues, aber es kommt dann doch immer wieder vor. Anhänge werden geöffnet oder man klickt auf Links und schon zeigt die Phishing-E-Mail ihre volle Wirkung. Ein Mensch ist neugierig!
   Was kann helfen? Regelmäßige Schulungen, klare Verhaltensregeln. Es geht nicht darum die Neugierde zu zügeln. Es geht darum, dass man das Gespür entwickelt, was vielleicht nicht so ganz passt.
3. Software, die veraltet ist
   Auch das sollte man mittlerweile wissen. Software-Updates sollten schnellstmöglich eingespielt werden. Cyberkriminelle nutzen bekannte Schwachstellen.
   Und hier? Auch, wenn dies eine Kernaufgabe der Geschäftsführung mit ihrer IT-Abteilung ist, so schadet es nicht, wenn Mitarbeiter auf Meldungen oder Hinweise auf ihrem System achten.
4. Ignoranz
   Menschen ignorieren manchmal gerne. So auch organisatorische und technische Vorgaben. Sie versuchen es zumindest bspw. in Stress-Situationen. „Ich habe gerade nicht die Zeit, ich mache es später.“ Es ist gar nicht einmal Vorsatz, es ist „Menschsein“.
   Kann hier etwas helfen? Den Mitarbeitern muss klargemacht werden, dass sie mitverantwortlich sind. Gem. der DSGVO müssen bspw. alle Mitarbeiter auf das Datengeheimnis verpflichtet werden. Einfach „Augenschließen“ ist

Impressum:
DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

keine Option.

5. Download aus unsicheren Quellen
   Es war und ist noch immer ein hohes Risiko, wenn Software oder Dateien aus unsicheren oder nicht verifizierten Quellen heruntergeladen wird. Das Risiko ist vielleicht höher als je zuvor. Immer mehr Apps kommen auf den Markt. Abhilfe? Die Technik muss in erster Linie so eingestellt werden, dass keine Downloads aus unbekannten Quellen möglich sind. Auch muss über mögliche Genehmigungsverfahren nachgedacht werden.

Löschkonzept nicht da. Bußgeld droht!

Es kommt immer häufiger vor. Unternehmen geraten ins Visier der Datenschutzaufsichtsbehörden. Hierbei wird u.a. festgestellt, dass das Unternehmen sich keine bzw. keine ausreichenden Gedanken zum Löschen von personenbezogenen Daten gemacht hat. Fakt, ein Löschkonzept liegt nicht vor. Die Folgen sind in der Regel erheblich, wenn bei einer Aufsichtsprüfung die Frage nach eben den Aufbewahrungsfristen zum Löschen gestellt wird, und man hat keine Antwort.

Und nun? Was sollte ein Unternehmen beachten?
Jedes Unternehmen muss wissen, wo welche Daten zu welchem Zweck gespeichert werden. Und wann eben diese auch wieder gelöscht werden müssen.
Wenn es noch keine Klarheit über Aufbewahrungsfristen gibt, dann mal los. Bevor Ihnen diese Frage durch eine Aufsicht gestellt wird.
Noch besser, Systeme überwachen automatisch die Fristen. Ganz ehrlich, Menschen vergessen halt gerne und verschieben, weil andere Dinge gefühlt wichtiger sind. Eine technische Unterstützung ist hier sehr hilfreich.

Fazit?
Egal, wie man das Thema angeht, es sollte dokumentiert sein. So kann man nachweisen, welche Gedanken man sich zu diesem Thema gemacht hat. Man zeigt zumindest das, was man machen möchte und bestenfalls bereits umsetzt. Keine Dokumentation bedeutet, dass auch nichts da ist.

KI für Cyberangriffe

Die KI birgt eine Vielzahl von Möglichkeiten. Aber manche können enorme Schäden nach sich ziehen.
ChatGPT bspw. unterstützt u.a. Programmierer beim Schreiben von Code. Aber auch Hacker!
Wenn man den Experten Glauben schenken kann, dann hat ChatGPT das Potenzial unerkennbaren Schadcode zu schreiben.

Zeit- und Aufwandsersparnis? Bei KI ein enormer Vorteil.
Für Cyberkriminelle ist es wichtig, dass eine Phishing-E-Mail glaubwürdig ist. Und je mehr dies der Fall ist, je größer die Chance, dass die Menschen darauf hineinfallen. Und auch das schafft KI, das Aussehen zu optimieren.

Impressum:
DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

Typische Kennzeichen einer schlechten Phishing-E-Mail?
Ja, mittlerweile bekannt. U.a. schlechtes Deutsch, falsche Grammatik oder die Rechtschreibung passt nicht. Aber auch die Persönlichkeit fehlt. Und eben diese Schwächen kann KI ausmerzen. KI lernt stetig und verbessert sich. Mails mit dem Ziel eines Datenabgriffs werden perfekt(er).
Fazit? Für uns Menschen wird es immer schwieriger eine Phishing-E-Mail zu erkennen. Mit der Folge, dass bspw. Zugangsdaten oder andere sensiblen Informationen abgegriffen werden. Und schon ist die Datenpanne da.

KI sammelt stetig!
Schon erwähnt, KI perfektioniert sich stetig. Profile werden gescannt, so dass die KI zielgerichtete perfekte Aufforderungen versendet, die echt aussehen.
Man erhält bspw. eine E-Mail von einer bekannten Person eines Dienstleisters. Und hier wird ein Ereignis angesprochen, welches wirklich stattfindet bzw. stattgefunden hat. Je ach Ereignis kommt es dann zu Handlungsaufforderungen. KI kann „guten“ Text schreiben UND Personen „nachbauen“. Zumindest in ihrem Verhalten.

Gibt es dann überhaupt Schutz?
Schon seit jeher klar, einen sicheren Schutz gibt es nicht. Auch nicht vor KI-basierten Cyberangriffen. Das Zusammenspiel einer Vielzahl von Maßnahmen ist hier wichtig. Hierunter fallen, auch hier wieder, stetige Awareness-Trainings oder auch Schulungen. Von Seiten der Technik sind Firewalls und Virenschutzsystem, aber auch Multi-Faktor-Authentifizierung und Zugangskontrollen ein Muss.

Multi-Faktor-Authentifizierung (MFA). Die Rettung?!

Ein Schutzfaktor, wie bspw. „Benutzername und Passwort“ ist gut, zwei Schutzfaktoren sind aber besser.
Was kann ein zweiter Faktor sein?

- Authenticator-App
- SMS
- E-Mail
- Anruf
- Hardwaretoken

Nun ist zu beobachten, dass mit zunehmender Nutzung von MFA auch die Angriffsszenarien sich verändern. Cyberkriminelle versuchen natürlich auch diesen Schutz zu knacken.
Bedeutet, dass eine MFA eine gute zusätzliche Absicherung für ein Unternehmen ist. Gem. einer Anforderung gem. der DSGVO ist es auch ein Muss für Unternehmen stetig die Schutzmaßnahmen anzupassen und somit eben eine solche MFA einzuführen.
Aber sich darauf ausruhen ist auf keinen Fall zu empfehlen.

Impressum:
DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

HINGESCHAUT
Datenschutz im Blick

Ransomware-Attacke? So etwas möchte man nicht!

Mittlerweile weiß man, was dahintersteckt. Das macht aber das Ganze auch nicht besser. Es gibt Möglichkeiten zur Risikoreduktion, die man, insbesondere Unternehmen, überlegen sollten, wie bspw.:

- Netzwerksegmentierung
- Sicherheitsüberprüfung
- Anwendungssicherheit
- E-Mail-Sicherheit
- Endpoint-Sicherheit
- Zugriffskontrolle
- Monitoring und Incident Response
- Sicherheitsschulungen
- Datensicherung

Es gibt ein paar Stellschrauben, um Ihre Sicherheit zu erhöhen! Wichtig dabei ist, dass sich Unternehmen mit der IT ein Gesamtkonzept überlegen, da die IT an jeder Stelle dabei ist. Auch spielt natürlich eine große Rolle wie das Unternehmen aufgestellt ist. Ist es sehr Cloud-lastig oder liegen die Daten eher im Unternehmen? Auch spielt u.a. die Branche eine große Rolle. Mitarbeiterinnen und Mitarbeiter sind ggf. dauerhaft unterwegs und nutzen andere Netze.

Cyberattacken aus September 2023 in Deutschland *(Textliche Auszüge aus www.dsgvo-portal.de)*

Vorab, es geht hier nicht ums „Angstmachen“. Vielmehr ist das Ziel die Sensibilisierung
→ „*So etwas ist ja auch bei uns vorgekommen*.“

- Motel One
  Hacker stehlen Kundendaten.
- Lok Leipzig
  Fußballverein muss nach Cyberangriff den Shop vom Netz nehmen
- Volkswagen
  Werke stehen nach IT-Störung still
- Kreditanstalt für Wiederaufbau (KfW)
  Website zur Beantragung von Fördergeldern nicht mehr erreichbar
- ADAC
  IT-Angriff auf die Infrastruktur

Impressum:
DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

HINGESCHAUT
Datenschutz im Blick

Europäische Bußgelder im September 2023? *(Textliche Auszüge von Dr-Datenschutz)*

Es ist nur eine **kleine** Übersicht! Aber es sind praxisnahe Fälle, die ggf. auch bei Ihnen auftreten können.

- Unzureichender Schutz der Daten von Minderjährigen
  Behörde: An Coimisiún um Chosaint Sonraí Data Protection Commission
  Branche: Soziale Netzwerke
  Verstoß: Art. 5 Abs. 1 a) DSGVO, Art. 5 Abs. 1 c) DSGVO, Art. 5 Abs. 1 f) DSGVO, Art. 12 Abs. 1 DSGVO, Art. 13 Abs. 1 e) DSGVO, Art. 24 Abs. 1 DSGVO, Art. 25 Abs. 1 DSGVO, Art. 25 Abs. 2 DSGVO
  Bußgeld: 345.000.000 Euro
- Verarbeitung von Gesundheitsdaten ohne Rechtsgrundlage
  Behörde: Agencia Española de Protección de Datos
  Branche: Sport, Gesundheitsdaten
  Verstoß: Art. 9 DSGVO, Art. 13 DSGVO
  Bußgeld: 17.000 Euro
- Weitergabe des Duplikats einer SIM-Karte an einen Betrüger
  Behörde: Agencia Española de Protección de Datos
  Branche: Kommunikationsunternehmen
  Verstoß: Art. 6 DSGVO
  Bußgeld: 80.000 Euro
- Verarbeitung von sensiblen Daten im Beschäftigungsverhältnis
  Behörde: Commission Nationale de l´Informatique et des Libertés
  Branche: Beschäftigtendatenschutz
  Verstoß: Art. 5 Abs. 1 lit. c DSGVO, Art. 9 DSGVO, Art. 10 DSGVO und Art. 31 DSGVO
  Bußgeld: 200.000 Euro
- Tonaufzeichnungen eines Vergewaltigungsopfers veröffentlicht
  Behörde: Agencia Española de Protección de Datos
  Branche: Weitergabe von personenbezogenen Daten
  Verstoß: Art. 5 Abs. 1 lit. c DSGVO
  Bußgeld: 50.000 Euro

Es geht nicht vorrangig um das Bußgeld. Auch nicht welche Behörde zuständig war. Die Unternehmen sollen sich hier bspw. die Fragen stellen: „Kann uns das auch passieren? Oder ist das auch bei uns so?“

Impressum:
DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT

Gesamtfazit?

Eine einhundertprozentige Sicherheit gab es in der Welt der IT noch nie. Wird es auch nie werden. Je digitaler ein Unternehmen ist, je mehr Risiko ist vorhanden. Und diesmal meine ich nicht nur die IT-Sicherheit, sondern auch den Datenschutz. Den Unternehmen muss klar sein, dass jede erfolgreiche Cyber-Attacke eine Datenpanne gem. der DSGVO darstellt.
Was kommt, wenn ein Unternehmen eine erfolgreiche Cyberattacke erlitten hat, ist nicht angenehm. Es ist Stress pur!
Wenn ein Unternehmen einen erfolgreichen Cyberangriff verbuchen muss, hat es in der Regel eine Vielzahl von Maßnahmen umzusetzen. Automatisch ist dann aber auch die Datenschutzaufsicht im Spiel, da es in der Regel auch um personenbezogene Daten geht. Hier gilt es den Schutz zu maximieren.
Unternehmen müssen, sofern sie es noch nicht machen, mit allen möglichen Schutzmaßnahmen auseinandersetzen.

Sie haben Fragen? Melden Sie sich bitte bei uns! Es bleibt spannend!

Was kommt in der nächsten Ausgabe von HINGESCHAUT?

Schauen wir mal. 😉
Ein Thema wird aber das **Aufzeichnen von Telefongesprächen** sein. Ist dies ok? Nicht ok? Darf man das?

Es bleibt spannend!

Anmerkung: Die Nichtnennung der 3 Personalformen (m, w, d) soll keine Diskriminierung darstellen, sondern lediglich die Lesbarkeit/Umfang verbessern.

Impressum:
DatCon GmbH | Ingenieurbüro für Datenschutz & Beratung, Am Osterfeuer 26, 37176 Nörten-Hardenberg
Kontakt: Fon 05503-9159648 | Fax 05503-9159649 | Mobil 0170-8162619 | Mail sorge@DatCon.de | Web www.DatCon.de

DATENSCHUTZ • UNTERNEHMENSBERATUNG • AUDIT • IT • GUTACHTEN • QUALITÄTSMANAGEMENT