**Musterfall: E-Mail-Konto wurde gehackt**

Ein Hackerangriff kann jeden treffen. Auch Handwerksunternehmens bleiben vor diesen Angriffen immer weniger verschont. *„Bei mir gibt es doch nichts zu holen“* – doch diese Denkweise ist falsch. Darum geht es nicht.

**Virtueller Einbruch**

Es muss ja nicht gleich ein Daten-Wiederherstellungs-Erpressungsversuch sein. Es reicht schon, dass der Betrieb mangels Zugriff auf eigene Daten durch einen Hackerangriff verwehrt wird oder gar verschwunden sind. In solchen Fällen wird die Wiederherstellung der Daten gegen Lösegeld erpresst oder zu mindestens versucht. Es reicht auch aus, dass z.B. ein Firmen-E-Mail-Account gekapert wurde.

Virtuell in ein Unternehmen einzubrechen, geht heute schneller als früher. Auch wenn die Daten auf einen Server im Betrieb und/oder über eine externe Sicherung doppelt gesichert sind, bleiben Unternehmen angreifbar.

Der Abschluss einer gesonderten Cyber-Versicherung wird daher auch für Handwerksunternehmen heute immer wichtiger. Auch hier hat der FHR für seine Mitglieder einen wichtigen Cyber-Sicherheits-Rahmenvertrag mit der HDI abgeschlossen.

**Ein Angriff aus Sicht der DSGVO**

Doch wie ist ein Angriff aus Sicht der DSGVO zu werten und welche Maßnahmen sind konkret erforderlich? Im Artikel „Datenschutzverstoß – was jetzt?“ wurde bereits darauf hingewiesen, dass eine Datenschutzvorfall auf jeden Fall zu dokumentieren und im Zweifel auch zu melden ist. Selbst bei kleinen Handwerksunternehmen liegt der einfache Tagessatz einer DSGVO-Strafe bei 972 € - und dieser Satz kann – je nach Schwer des DSGVO-Verstoßes – mit einem Mulitplikator von 12 versehen werden.

Es wird dabei nicht der Hacker-Angriff als solcher bestraft, sondern hier ggf. eine fehlende Umsetzung der DSGVO in ein betriebliches Gesamt-Daten-Sicherungskonzept. Und es spielt dabei auch eine Rolle, ob ein Datenschutzvorfall „sauber“ dokumentiert und im Anschluss abgewogen wurde, ob es sich bei dem konkreten Fall um einen Meldepflichtigen Vorgang handelt.

**Die Uhr tickt: 72-Stunden**

Ein *meldepflichtiger* Datenschutzvorfall soll unverzüglich, möglichst jedoch binnen 72 Stunden bei den Aufsichtsbehörden gemeldet werden (Art. 33 Abs. 1 DSGVO). Unabhängig davon, ob es sich um einen meldepflichtigen Vorgang handelt, sind alle Datenschutzvorfälle jedoch zu dokumentieren. Im Rahmen einer solchen Dokumentation ist eine Bewertung des Datenschutzvorfalles vorzunehmen.

**Fallbeispiel:**

Am Morgen des 11.01.2022 stellt der Geschäftsführer eines Unternehmens fest, dass von seinem E-Mail-Konto versucht wurde, Spammails zu versenden. Hierauf wurde durch die IT-Abteilung die Passwörter geändert. Kurze Zeit später erhält der Geschäftsführer einen Anruf von einer Kundin, dass diese von ihm eine „seltsame E-Mail“ erhalten hat und bittet um Prüfung. Die Prüfung hat nun ergeben, das tatsächliche einzelne Mails an Kunden versendet worden sind.

Was ist nun zu tun?

Zweifellos handelt es sich hier um einen datenschutzrelevanten Vorgang. Dieser ist als solcher im Rahmen des (hoffentlich bestehenden) Datenschutzkonzeptes des Unternehmens zu dokumentieren und im Anschluss zu beurteilen, ob dieser Vorgang so schwer wiegt, dass dieser auch der zuständigen Datenschutzbehörde zu melden ist.

**Wie eine solche Dokumentation aussehen kann, zeigt folgendes Beispiel:**

**Musterfall: Dokumentation eines IT–Sicherheitsvorfalls: Beispiel: E-Mail gehackt**

1. **Kurzbezeichnung, Datum und Uhrzeit des Sicherheitsvorfalls:**

Am **11.01.2022** um **8:50** Uhr wurde das E-Mail-Konto [**m.mustermann@muster-gmbh.de**](mailto:m.mustermann@muster-gmbh.de) gehackt.

1. **Angaben zum Verfasser des Protokolls/Protokolls:**

**Interne Datenschutzbeauftragte: Maria Müller**

1. **Involvierte und Verantwortliche:**

* **Involvierte: Max Mustermann (Geschäftsführer)**
* **Verantwortliche: Maria Müller**

1. **Beschreibung des IT-Sicherheitsvorfalls**

**4.1 Was ist vorgefallen?**

Am **11.01.2022** um **8:50** Uhr sind von der E-Mail-Adresse [**m.mustermann@muster-gmbh.de**](mailto:m.mustermann@muster-gmbh.de) Spam-Emails an für uns unbekannte E-Mail-Adressen gesendet worden. Unser Office 365 (Outlook) hat dies, nach unserem Stand, aber komplett unterbunden.

Am **11.01.2022** um **9:25** Uhr meldeten wir dies an unsere IT-Firma und diese änderten das Passwort für die angegriffene E-Mail-Adresse. Gegen **10:45** Uhr am **11.01.2022** wurden wir dann von einer Kundin über eine Spamnachricht im Namen von [**m.mustermann@muster-gmbh.de**](mailto:m.mustermann@muster-gmbh.de) informiert. Diese wurde um **9:10** Uhr versendet.

**E-Mail: Spamtext**

**4.3 Was war die Ursache des Vorfalls?**

* Diebstahl
* **Hacking / Ausspähung von Daten**
* Betrug
* Sabotage
* Informationsabfluss
* nicht autorisierte Verwendung von Ressourcen
* Physikalische Beschädigung
* Hardware-Fehler
* Software-Fehler
* Netzwerk-Fehler
* Personalknappheit
* Feuer
* Wasser
* andere natürliche Ereignisse
* Systemausfall
* Fehlbedienung
* Planungsfehler
* **Welche Systeme/Komponenten sind betroffen?**

**E-Mail-Account über Office 365 (Outlook)**

* **Welche negativen Auswirkungen auf Geschäftsprozesse sind die Folge?**

**Keine Auswirkungen, lediglich Behebung Aufwand durch Erhöhung der internen Sicherheitsstruktur und Fehlerbehebung**

* **Welche Schwachstellen wurden identifiziert?**

**Einfache Passwortregelungen, die zu wenig verändert wurden**

**4.4 Datum und Uhrzeit des Eintritts, der Erkennung und der Meldung des IT-Sicherheitsvorfalls:**

Eintritt: Am **11.01.2022** ab **8:50** Uhr

Erkennung: Am **11.01.2022** um **9:10** Uhr

Meldung an IT-Firma: Am **11.01.2022** um **9:25** Uhr

**4.5 Ist der IT-Sicherheitsvorfall abgeschlossen? Wenn NEIN, wie lange dauert der IT-Sicherheitsvorfall bereits an?**

**JA, IT-Firma hat Passwörter geändert.**

**4.6 Beschreibung der betroffenen Komponenten (z. B. Informationen/Daten, Hardware, Software, Kommunikationssysteme, Dokumente, betroffene Kunden usw.):**

**E-Mail-Adresse von** [**m.mustermann@muster-gmbh.de**](mailto:m.mustermann@muster-gmbh.de) **im System Outlook**

**4.7 Auswirkungen des IT-Sicherheitsvorfalls**

* Finanzieller Verlust
* **Störung von Geschäftsprozessen**
* **Preisgabe personenbezogener Daten (nur E-Mailadressen)**
* Verstoß gegen gesetzliche und behördliche Verpflichtungen

**4.8 Beschreibung der Auswirkungen:**

Versand von Spam-Emails an Kontakte von [**m.mustermann@muster-gmbh.de**](mailto:m.mustermann@muster-gmbh.de)

**5.0 Durchgeführte Maßnahmen:**

* **Änderung der Passwörter**
* **Meldung an die Polizei**
* Information an relevante Kunden

**6.0 Geplante Maßnahmen:**

**Verschärfung der Passwortsicherheit**

**7.0 Geschätzte Gesamtkosten für die Bewältigung des IT-Sicherheitsvorfalls:**

**Nicht einschätzbar, da alle Kosten über den Servicevertrag mit unserer IT-Firma laufen**

**Zusammenfassende Bewertung des IT-Sicherheitsvorfalls:**

Eine Risikoidentifikation deutet neben der Identifikation möglicher Risiken auch auf die Risikobewertung (Beurteilung der Schwere des Schades) sowie auf die Eintrittswahrscheinlichkeit hin. Hieraus sind dann ggf. Präventionsmaßnahmen zu ergreifen.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Risikofaktoren lt. ErwGr 75**  **(Erwägungsgründe lt. DSGVO)** | **Schwere des Schadens**  **(A)** | **Eintrittswahrscheinlichkeit**  **(B)** | **Risikograd**  **(A x B)** | **Präventions-**  **maßnahmen** |
| *1.* | physischer, materieller oder immaterieller Schaden | 1 | 1 | 1 | TOM |
| *2.* | Diskriminierung, Identitätsdiebstahl oder -betrug | 2 | 1 | 2 | TOM |
| *3.* | Finanzieller Verlust | 1 | 1 | 1 | TOM |
| *4.* | Rufschädigung | 2 | 1 | 2 | TOM |
| *5.* | Verlust der Vertraulichkeit der dem Berufsgeheimnis unterliegenden personenbezogenen Daten | 1 | 1 | 1 | TOM |
| *6.* | Aufhebung der Pseudonymisierung | / | / | / | Nicht relevant |
| *7.* | erhebliche wirtschaftliche oder gesellschaftliche Nachteile | 2 | 1 | 2 | TOM |
| *8.* | Verlust o. Beschränkung von Rechten | / | / | / | Nicht relevant |
| *9.* | unerlaubte Verarbeitung von besonderen Kategorien pers.bez.Daten (Art. 9 DSGVO) | / | / | / | Nicht relevant |
| *10.* | Bewertung persönlicher Aspekte, wie z.B. Arbeitsleistung, wirtschaftliche Lage, Gesundheit | / | / | / | Nicht relevant |
| *11.* | Bewertung persönliche Vorlieben oder Interessen, der Zuverlässigkeit, das Verhalten oder den Aufenthaltsort | / | / | / | Nicht relevant |
| *12.* | Erstellung persönlicher Profile | / | / | / | Nicht relevant |
| *13.* | Verarbeitung von personenbezogenen Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern | / | / | / | Nicht relevant |
| *14.* | Verarbeitung einer großen Menge personenbezogener Daten | / | / | / | Nicht relevant |

* *TOM Technisch – organisatorische Maßnahmen*

**Mögliche Einteilung einer Risikobewertung**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bewertung** | **Auswirkung auf den Betroffenen** | **Folgen überwinden können** | **Beispiele** |
| **1. Gering** | Nicht betroffen oder nur geringe Unannehmlichkeiten | Unannehmlichkeiten sollten sich problemlos beheben lassen | Zeitverlust, Irritationen usw. |
| **2. Mittel** | Wesentliche Unannehmlichkeiten | Unannehmlichkeiten sollten sich – trotz gewisser Schwierigkeiten – überwinden lassen | Stress, Vertrauensverlust, Angst usw. |
| **3. Hoch** | Wesentliche Folgen | Folgen sollten sich – trotz gewisser Schwierigkeiten – überwinden lassen | Finanzieller Verlust, Erheblicher Imageschaden, negative Auswirkung auf Gesundheit usw. |
| **4. Sehr hoch** | Wesentliche und/oder nicht umkehrbare Folgen | Folgen lassen sich kaum oder gar nicht überwinden | Erheblicher finanzieller Verlust, Arbeitslosigkeit, langfristige negative Auswirkungen auf Gesundheit usw. |

**Mögliche Einteilung einer Eintrittswahrscheinlichkeit**

|  |  |  |
| --- | --- | --- |
| **Bewertung** | **Realisierbarkeit der Bedrohung** | **Beispiele** |
| **1. Gering** | Mit hoher Wahrscheinlichkeit nicht möglich | Diebstahl von Dokumenten / Daten aus einem gesicherten Raum / Tresor (Schutz durch Zugangscode), z.B. Serverraum / Verschlüsselung von Daten durch BitLocker sowie Verschlüselung von Daten innerhalb der Cloud./ Spammails |
| **2. Gelegentlich** | Schwierig und nur mit großem Aufwand möglich | Diebstahl von Dokumenten / Daten aus einem gesicherten, abgeschlossenen Raum (kein Schutz durch Zugangscode) |
| **3. Häufig** | Machbar, selbst mit geringem Aufwand | Diebstahl von Dokumenten / Daten aus einem zugänglichen Büro |
| **4. Sehr häufig** | Einfach | Diebstahl oder Verlust von Dokumenten / Daten, die nicht gesondert gesichert sind. |

Der Risikograd wird durch die Multiplikation der Schwere des Schadens und der Eintrittswahrscheinlichkeit ermittelt. Hieraus lässt sich dann eine Risikomatrix erstellen. Die einzelnen Felder der Matrix gehören zu einem bestimmten Risikobereich.

Aus einer einfachen Farbgestaltung werden die Risikobereiche deutlich gekennzeichnet und können ggf. nach Prioritäten bearbeitet werden.





**Eintrittswahrscheinlichkeit**

**Allgemeine Leitlinien:**

Im Unternehmen besteht folgende Leitlinie zur Behandlung der Risiken:

1. Angestrebtes Ziel ist die Eliminierung der erkannten Risiken.
2. Es werden regelmäßige Prozesse initiiert, um die gelegentlich auftretenden Risiken zu erkennen und zu eliminieren.
3. Wenn die Risiken häufig auftreten und die Reduzierung technisch nicht machbar ist oder nur durch zu hohen Aufwand realisiert werden kann, wird eine Minimierung des Risikos angestrebt.
4. Wenn das Risiko nicht minimiert werden kann, wird die Aufsichtsbehörde informiert.

**Risikobewertung zum Sicherheitsvorfall:**

1. Wir bewerten den Sicherheitsvorfall als **geringes Risiko**, da nur Emailadressen abgefangen wurden. Die versendeten E-Mails enthielten nach unserer Vermutung keinen Link oder Geldforderungen. Die versandte E-Mail ist in der Kennung als Spam deutlich erkennbar.
2. Eine Verwundbarkeit des Office 365 (Outlook) / Exchange Servers war zwar gegeben, jedoch kann eine Kompromittierung nach unserer Ansicht ausgeschlossen werden. Es wurden intern weitere Schutzmaßnahmen durchgeführt, die ein weiteres mögliches Eindringen verhindern. Nach Durchführung der Sicherheitsmaßnahmen wurden von eigenen Mail-Server keine weiteren Mails versandt; zudem haben auch wir selbst keine Mails erhalten. Informationen von Kunden lagen ebenfalls nicht vor.
3. Es kann aus unserer Sicht ein Risiko für die betroffenen Personen nach DSGVO ausgeschlossen werden. Es liegt somit keine meldepflichtige Datenschutzverletzung vor, da der Vorfall voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (vgl. Art. 33 DS-GVO).

**Fazit:**

**Die Risikobewertung zeigt, dass die relevanten Risikofaktoren und Bewertungen insgesamt im „grünen Bereich“ befinden. Es liegt somit keine meldepflichtige Datenschutzverletzung vor.**

Ort, Datum Verantwortlicher (Unterschrift)

**Meldung des Datenschutzvorfalles**

Im vorliegenden Fall war nach interner Prüfung des eine Meldung des Datenschutzvorfalles nicht notwendig. Bei einem schwerwiegenderen Fall – wie beispielsweise einem Diebstahl aller Kundendaten – wäre eine Meldung zwingend erforderlich gewesen.

Wie eine solche Meldung aussehen kann, zeigen wir in einem nächsten Newsletter auf.

**Wie unterstützt der FHR seine Partner in Sachen Datenschutz?**

**FHR-Rahmenvereinbarung DSGVO**

Für alle Unternehmen, die sich diesem Thema mit professioneller Unterstützung umfassend erstellen wollen, hat der FHR-Verbund mit dem Branchenexperten, Unternehmensberater und zertifzierten betrieblichen Datenschutzbeauftragten Dieter Perk, eine Rahmenvereinbarung geschlossen.

**Hotline DSGVO**

Diese Rahmenvereinbarung umfasst eine kostenlose Hotline DSGVO im Rahmen einer telefonischen Erstauskunft.

**Handbuch zur Umsetzung der DSGVO**

Für die Umsetzung hat er ferner ein Handbuch erstellt, welches zum FHR-Vorzugspreis von 499 € + MwSt. (regulär 599 €) erworben werden kann.

****