Computacenter

SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT – UMGANG MIT INFORMATIONEN

Informationen schützen

INFORMATIONEN SCHÜTZEN

Einführung

„Informationen schützen“

In diesem Abschnitt erfährst Du, warum der Schutz von Informationen so wichtig ist. Wir wollen Dir klarmachen, dass wir alle als Mitarbeiter von Computacenter Verantwortung dafür tragen, unsere sensiblen Informationen und andere Ressourcen des Unternehmens zu schützen.

Denke immer daran, dass Du beim Schutz von Informationen nicht auf Dich alleine gestellt bist. Die Experten des Information Security Management-Teams stehen bereit, um Deine Fragen zu beantworten, Dich zu beraten und unterstützen. Du brauchst Dich nur an die Group Information Assurance (GIA) wenden.

In unserem Arbeitsalltag müssen wir beinahe ständig mit Informationen umgehen. Informationen liegen in sehr unterschiedlicher Form vor und sind für Unternehmen sehr wertvoll. Sie sind auch eine der wertvollsten Vermögenswerte von Computacenter.

„Bei uns im Büro erledigen wir so gut wie alles per Computer. Heutzutage sind unsere gesamten Unternehmens- und Kundendaten dort gespeichert. Vor kurzem wurden alle in unserem Unternehmen von unserer IT-Abteilung dazu aufgefordert, unsere Kennwörter umgehend zu ändern. Es gab da ein Sicherheitsproblem.

Allein die Vorstellung, wir müssten unsere Kunden darüber informieren, dass ihre Daten nicht mehr sicher seien... das wäre ein derartiger Aufwand, und wir würden das gesamte Vertrauen unsere Kunden verlieren.“

„Du glaubst nicht, was alles offen auf den Schreibtischen herumliegt. Und wie viele vertrauliche Unterlagen einfach im Papierkorb landen! Ich mache hier ja nur die Büros sauber, aber ich könnte jeden Abend diverse E-Mail-Ausdrucke, Sitzungsprotokolle und andere Dokumente einsammeln. Niemand würde es merken oder vermissen. Die perfekte Wertstoffsammlung für Industriespione!“

„Als Servicetechniker bin ich für viele Unternehmen tätig, oftmals alleine und unbeaufsichtigt. Wenn ich wollte, könnte ich da ganz einfach ein linkes Ding drehen.

Wenn jemand vergisst seinen Computer zu sperren, brauch ich eigentlich nur einen USB-Stick mit Malware. Auch Haftnotizen mit Anmeldedaten oder vertrauliche Dokumente, die einfach so herumliegen, sind sehr hilfreich!

Dann einfach nur genüsslich zurücklehnen und zuschauen, wie das Chaos sich ausbreitet…“

Szenarien

Lässt sich aus den folgenden Aussagen ableiten, dass die Vertraulichkeit, Integrität und Verfügbarkeit der betroffenen Informationen beeinträchtigt wurde?

„Gestern Abend wurde mir in der Kneipe mein Laptop gestohlen. Auf ihm waren die Kontaktadressen aller meiner Kunden sowie die Angebote gespeichert, an denen ich gerade arbeite. Jetzt bereue ich es, dass ich kein starkes Anmeldekennwort festgelegt habe."

Vertraulichkeit -

Die Vertraulichkeit der Kundenkontakte und der Angebotsinformationen ist in Gefahr, weil ein schwaches Kennwort verwendet wurde, das einfacher zu erraten oder zu knacken ist..

„Gestern wurde eine Änderung an den IT-Systemen vorgenommen, ohne dabei den vorgeschriebenen Change Management-Prozess zu befolgen. Das führte dazu, dass unser E-Mail-Server den ganzen Tag außer Betrieb war."

Verfügbarkeit –

Die E-Mail-Funktion ist nicht verfügbar, wenn der Server außer Betrieb ist.

„Ich habe aus Versehen eine E-Mail mit den gesamten Lohnbuchhaltungsdaten (einschließlich der Gehälter) an das IT Service Desk anstatt an HR Service Desk (den eigentlichen Empfänger) gesendet."

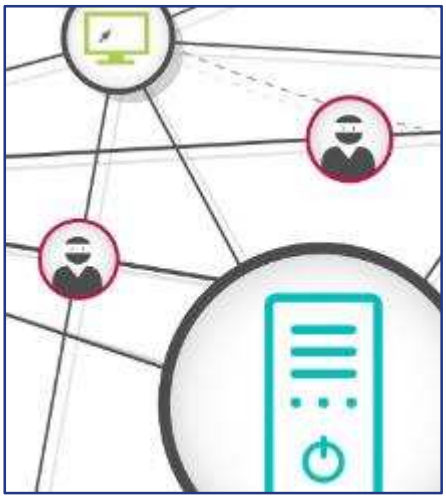
Vertraulichkeit –

Vertrauliche Informationen wurden an eine Abteilung gesendet, die nicht berechtigt ist, sie einzusehen. Dies stellt einen Bruch der Vertraulichkeit dar.

„Ein Hacker hat unser Netzwerk infiltriert und sämtliche Preisangaben auf unserer Webseite geändert. Das hat das Unternehmen eine Menge Geld gekostet, da wir mehrere Stunden lang PCs für nur einen Euro verkauft haben!"

Integrität –

Die Preisangaben auf der Webseite wurden geändert, was eine Verletzung der Integrität darstellt.



Digital vorgetragene Angriffe sind besonders gefährlich, da dabei sehr schnell riesige Datenmengen übertragen oder manipuliert werden können.

Wettbewerber, einzelne Kriminelle oder sogar Staaten haben starkes Interesse daran, sich Zugang zu unseren Daten zu verschaffen – entweder zum eigenen Nutzen oder um unserem Unternehmen zu schaden. Deshalb gibt es eine Vielzahl von Leitlinien, Auflagen und Gesetzen zum Schutz von Informationen.

Aber wer trägt letztlich die Verantwortung für die Einhaltung dieser Regeln?

☐ Die staatlichen Aufsichtsbehörden

☒ Die Unternehmen

☒ Jeder einzelne Mitarbeiter in seinem Bereich

Neben den Unternehmen trägt jeder einzelne Mitarbeiter in seinem Bereich die Verantwortung für die Einhaltung der Regeln.

Die staatlichen Aufsichtsbehörden sind nicht für die Einhaltung der Regeln in unserem Unternehmen verantwortlich, sie haben eine übergeordnete Kontrollfunktion.

Alle internen Unternehmensdaten müssen geschützt werden. Davon sind jedoch personenbezogene Daten noch einmal zu unterscheiden, da diese direkt oder indirekt einer Person zugeordnet werden können. Es spielt dabei keine Rolle, ob es sich um Kunden, Mitarbeiter, Geschäftspartner oder andere Personen handelt.

Vor kurzem hat es in Zusammenhang mit personenbezogenen Daten eine Gesetzesänderung gegeben. Am 25. Mai 2018 ist die neue, europaweit gültige Datenschutz-Grundverordnung (DSGVO) in Kraft getreten, die strikte Konsequenzen für Unternehmen vorsieht, die sich nicht an sie halten.

Computacenter stellt Schulungen zu den Anforderungen der DSGVO über das EnTras-Tool zur Verfügung. Alle Mitarbeiter sind verpflichtet, diese Schulung zu absolvieren (hierzu gehört auch, den kurzen Test am Ende zu bestehen).

Grundsätzlich gilt für alle Arten von Daten: Werden sensible Informationen im Unternehmen nicht ausreichend geschützt, drohen empfindliche Konsequenzen.

Welche Folgen hältst Du für möglich?

- ☒ Wirtschaftlicher Schaden durch den Verlust von exklusivem Know-how
- ☒ Wirtschaftlicher Schaden durch Rufschädigung
- ☒ Bußgelder für das Unternehmen
- ☒ Arbeitsrechtliche Konsequenzen für die verantwortlichen Mitarbeiter
- ☒ Schadenersatzforderungen durch Geschädigte

Du hast Dich in allen Fällen richtig entschieden. Sieh zusätzlich die weiterführenden Hinweise zu jeder Auswahl.

Option 1: Verliert z. B. ein Mitarbeiter einen USB-Stick mit exklusiven Forschungsergebnissen Ihres Unternehmens und sie gelangen zu einem Konkurrenten, ist der Wettbewerbsvorsprung verloren.

Option 2: Der Imageschaden für das Unternehmen ist oft die schwerwiegendste Folge, z. B. wenn von einem unzureichend geschützten Server die Kreditkartendaten von Kunden gestohlen werden.

Option 3: Nach Verstößen gegen die Datenschutzgesetze können die zuständigen Behörden empfindliche Bußgelder verhängen, z. B. wenn umfassende Kundenprofile mit Angaben zum Kaufverhalten ohne deren Zustimmung an ein anderes Unternehmen für Werbezwecke weitergegeben werden

Option 4: Auch dem einzelnen Mitarbeiter drohen Konsequenzen bei Verstößen gegen geltendes Datenschutzrecht. Arbeitsrechtliche Folgen (Ermahnung, Abmahnung oder auch Kündigung)

Option 5: Bei Verletzungen des Datenschutzes können Betroffene Schadenersatz einklagen.

Zusammenfassung

In diesem Abschnitt hast Du gelernt...

- dass der Schutz von Informationen für den Schutz und die Aufrechterhaltung unserer geschäftlichen Abläufe unerlässlich ist, da es sich um Vermögenswerte handelt.
- welche Konsequenzen es hat, wenn unsere Informationen nicht ordnungsgemäß geschützt werden.
- dass Du selbst Verantwortung zum Schutz unserer Informationen trägst.

<u>Datenschutzverletzungen und Informationssicherheitsvorfälle:</u>

Es könnte sich herausstellen, dass Informationen nicht ordnungsgemäß geschützt wurden (entweder beabsichtigt oder unbeabsichtigt). Hier einige Beispiele:

- Offenlegung von sensiblen/vertraulichen Informationen
- Diebstahl/Verlust von Geräten mit Daten bzw. unbefugter Zugriff darauf
- Modifizierung/Entfernen von Informationen.

In allen Fällen muss ein Informationssicherheitsvorfall über das NGSD gemeldet werden.