Computacenter

SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT – UMGANG MIT INFORMATIONEN

Mobiles Arbeiten

MOBILES ARBEITEN EITEN

EINFÜHRUNG

‚Mobiles Arbeiten Eiten‘

Hast Du schon einmal darüber nachgedacht, wie Dein Verhalten bei der Arbeit außerhalb des Büros die Sicherheit des Unternehmens beeinflussen könnte? In diesem Abschnitt zeigen wir Dir, wo die Gefahren lauern und wie Du Dich und Computacenter effektiv davor schützen kannst.

Szenarien

Nach einem längeren Meeting zur bevorstehenden Veröffentlichung eines neuen Produkts sind Samira und ihre Kollegen endlich gemeinsam auf dem Weg in die Mittagspause. In einem Bistro in der Nähe setzen sie sich an einen Tisch und geben ihre Bestellungen auf. Während sie auf ihr Essen warten, ist Zeit zum Plaudern.

Samira hat sich im Meeting geärgert und macht sich nun bei den Kollegen Luft. Es wird alles diskutiert: das neue Produkt, die vorgestellte Marketingstrategie und das Preismodell.

Was denkst Du über die Situation?

1. **Das ist kritisch, jemand könnte lauschen.**
2. **Das ist okay, solange kein Fremder zuhört.**
3. **Das ist kein Problem, das interessiert doch keinen Fremden.**

Die Situation beim Mittagessen war sehr kritisch.

Im Regelfall gilt, dass Informationen, die Computacenter betreffen, eigentlich nie in der Öffentlichkeit diskutiert werden sollten.

Warum? – Das ist einfach:

Solche Informationen sind sensibel und müssen geschützt werden, weil sie in den falschen Händen für uns einen wirtschaftlichen Schaden anrichten könnten.

Zwei beispiele:

- Nachteil bei Ausschreibung - Ein Mitarbeiter eines Konkurrenzunternehmens sitzt zufällig am Nachbartisch und belauscht das Gespräch. Die Informationen über das Preismodell gibt er an seinen Arbeitgeber weiter. Die Rückschlüsse, die sich aus dem Preismodell ziehen lassen, nutzt dieser für eine aktuelle Ausschreibung und bekommt dadurch den Zuschlag.

- Schlagzeilen in der Presse - Ein „Mithörer“ belauscht das Gespräch und gibt die Informationen über unser neues Produkt, unser Preismodell und vor allem „die Gesprächssituation“ an die Presse weiter. Nicht nur Negativschlagzeilen, weil vertrauliche Informationen öffentlich besprochen wurden, sondern auch ein immenser Reputationsverlust sind die Folge.

Diebstahl/Liegenlassen

Mobiltelefone, Laptops und andere Mobilgeräte sind insbesondere unterwegs Risiken ausgesetzt, da sie leicht gestohlen oder liegengelassen werden (z. B. in einem Taxi).

Unbefugte, die über die Schulter bei Dir mitlesen

Auf Geschäftsreise kommt es häufig vor, dass man die Zeit nutzt und im Zug arbeitet. Du solltest dabei darauf achten, dass Unbefugte Deine Dokumente oder Deinen Bildschirm nicht einsehen können.

Possible damage

War das Gerät nicht gesperrt, hat der Dieb möglicherweise ungehinderten Zugriff auf geschäftliche Informationen wie Namen, Telefonnummern, Nachrichten und E-Mails.

Ein Hacker könnte sich Zugang zum Unternehmensnetzwerk und den dort gespeicherten Daten verschaffen.

Was tun bei Verlust?

Diebstahl oder Verlust von Laptops und Mobilgeräten sind umgehend zu melden.

Nur so lassen sich alle davon möglicherweise betroffenen Accounts unverzüglich sperren, um den möglichen Schaden zu begrenzen!

Wenn die Festplatte oder der Speicher nicht verschlüsselt sind, können auch die Daten eines ausgeschalteten Geräts ausgelesen werden.

Aus diesem Grund musst Du umgehend einen Informationssicherheitsvorfall über das NGSD melden, damit mit potenziellen Risiken auf geeignete Weise umgegangen wird.

Es hat sich außerdem bewährt, nur dann Daten auf der Festplatte zu speichern, wenn dies unbedingt erforderlich ist (z. B. wenn keine Netzwerkverbindung möglich ist). Auf einem Mobilgerät gespeicherte Daten sollten so schnell wie möglich entweder nach SharePoint oder OneDrive verschoben und dann vom Gerät gelöscht werden.

Die Daten auf unternehmenseigenen Laptops werden zwar verschlüsselt, dazu muss der Laptop aber erst heruntergefahren werden. Vergewissere Dich deshalb, dass Du Deinen Laptop herunterfährst, wenn Du ihn nicht mehr brauchst.

Was kannst Du tun, damit die Informationssicherheit gewahrt wird?

Ich sollte in der Öffentlichkeit…

… einen Blickschutzfilter benutzen.

… meinen Laptop oder mein Mobiltelefon nicht unbeaufsichtigt lassen.

… vertrauliche Dokumente nicht für jeden sichtbar herumliegen lassen.

… das Handy nach dem Telefonat sperren.

… auf die Bearbeitung von vertraulichen Dokumenten verzichten.

Alle Maßnahmen sind dazu geeignet, Deine Informationen in der Öffentlichkeit zu schützen. Geize bitte nicht damit.

Denke bitte daran, dass auch wenn Du **von zuhause aus arbeitest**, trotzdem dieselben Anforderungen an die Informationssicherheit gelten. Du musst dafür sorgen, dass ein angemessener Arbeitsplatz zur Verfügung steht und Dritte Informationen auf Deinem PC nicht einsehen bzw. darauf zugreifen können. Außerdem muss eine sichere Verbindung (VPN) zum Computacenter-Netzwerk bestehen, bevor Du auf Computacenter-Informationen zugreifst bzw. mit diesen arbeitest.

Mitarbeiter, die von zuhause aus im Kunden-Support arbeiten, müssen über sämtliche geltenden Vorschriften für den Remote-Zugriff auf die Kundenumgebung unterrichtet sein und sich an diese halten.

Zusammenfassung

In diesem Abschnitt...

- hast Du gelernt, dass beim Austausch von Informationen in der Öffentlichkeit Vorsicht geboten ist.
- hast Du einige Tipps erhalten, wie Du Dich in der Öffentlichkeit verhalten solltest, um sensible Unternehmensdaten zu schützen.
- hast Du gelernt, was zu tun ist, wenn Dir Dein Mobilgerät gestohlen wurde oder abhandengekommen ist.
- wurdest Du darauf hingewiesen, dass Du es vermeiden solltest, Daten auf die Festplatte zu speichern.
- hast Du gelernt, dass die Vorschriften für die Informationssicherheit auch für die Arbeit von zuhause aus gelten.

Datenschutzverletzungen und Informationssicherheitsvorfälle:

Wenn Dir IT-Geräte abhandengekommen sind oder gestohlen wurden oder Du glaubst, dass Informationen möglicherweise in die falschen Hände geraten sein könnten, melde bitte umgehend einen Informationssicherheitsvorfall über das NGSD.