Computacenter

SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT – UMGANG MIT INFORMATIONEN

Elektronische Kommunikation

ELEKTRONISCHE KOMMUNIKATION

Einführung

‘Elektronische Kommunikation’

In diesem Abschnitt erfährst Du, wie Du Risiken bei der Nutzung von **E-Mail & Kommunikation** sowie **Internet & Cloud** vermeidest und was Du bei der Nutzung sozialer Medien bedenken solltest..

Hast Du heute schon eine E-Mail gelesen, mit Deinem Handy telefoniert oder eine Kurznachricht geschrieben?

In diesem Augenblick passiert diese Art der Kommunikation millionenfach und kaum ein Alltag ist heute noch ohne E-Mails, SMS, Kurznachrichten, Chats, Foren, Faxe, Drucker, Handys, Tablets und Laptops denkbar.

Doch jedes Mal, wenn Du etwas elektronisch übermittelst oder empfängst, gibt es Gefahren. Jemand könnte mitlesen oder mithören, Nachrichten manipulieren, schadhafte Programme anhängen, Spionageprogramme einschleusen und vieles mehr.

Email

Zunächst geht es um E-Mails, sowohl privat als auch geschäftlich weiterhin eines der beliebtesten und wichtigsten Mittel zur Verständigung. Allerdings sind sie auch bei Kriminellen beliebt. Millionenfach verschickte Spam-Mails mit unerwünschter Werbung sind eher lästig.

Gefährlich wird es allerdings, wenn über Mail-Anhänge oder Links Schadsoftware eingeschleust wird oder über gefälschte Internetseiten Kennwörter oder Zugangsdaten gestohlen werden. Man spricht hier auch von „Phishing“.

Leistungsfähige Spam-Filter im Mail-Programm fangen einen Großteil der verdächtigen Post ab. Aber der Schutz kann nie hundertprozentig sein. Bleibe deswegen trotz der täglichen Mail-Flut aufmerksam – achte auf unbekannte Absender und insbesondere auf Links und Anhänge, deren Zweck Du nicht kennst.

Vorsicht im Umgang mit E-Mails!

- Lästig: Spam-Mails mit unerwünschter Werbung
- Gefährlich: wenn über Mail-Anhänge oder Links Schadsoftware eingeschleust wird

- Gefährlich: wenn über gefälschte Internetseiten Kennwörter oder Zugangsdaten gestohlen werden („Phishing“)

Szenarien

Entscheide bitte für jede Aussage.

Handelt es sich um einesinnvolle Verhaltensregel für den Umgang mit E-Mails?

Ja	Nein	
◉	○	Wenn ich den Absender nicht kenne, klicke ich in der E-Mail weder auf einen Link noch öffne ich einen Anhang.
◉	○	Selbst wenn ich den Absender kenne, wenn mir der Betreff der E-Mail verdächtig vorkommt oder unerwartet ist, halte ich mit dem Absender Rücksprache, bevor ich die Mail oder Anhänge öffne
◉	○	Fordert mich eine E-Mail zur Eingabe vertraulicher Daten auf, werde ich grundsätzlich misstrauisch und folge der Aufforderung nicht.
◉	○	Wenn die E-Mail, die ich erhalten habe, unangemessene Inhalte wie diskriminierende, obszöne oder diffamierende Informationen enthält, sollte ich dies meinem Vorgesetzten melden.

Öffne eine Mail mit merkwürdigem Betreff besser nicht - der Header bzw. die Absenderinformation könnte gefälscht sein. Aber an die anderen Regeln solltest Du Dich tatsächlich halten.

Unverschlüsselte Daten sind dort offen lesbar, wie eine normale Postkarte.

Streng vertrauliche Information müssen **verschlüsselt** werden, bevor sie an einen Empfänger außerhalb des Unternehmensnetzwerks geschickt werden.

Die Informationen sollten in einem passwortgeschützten Anhang gesendet werden (wobei das zugehörige Passwort über ein anderes Medium, z. B. per Telefon) übermittelt werden sollte).

Auch unterwegs ist es heute fast überall selbstverständlich, über ein Telefonnetz oder W-LAN auf Daten und E-Mails zuzugreifen.

Achtung: Per Funk übermittelte Daten können von Dritten empfangen, aufgezeichnet und sogar manipuliert werden

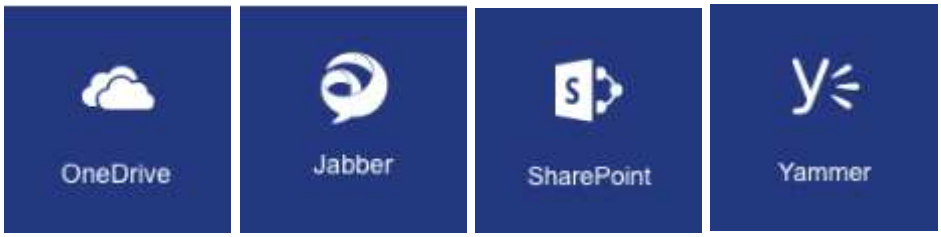
Um sich davor zu schützen, …

… muss der Remote-Zugriff auf das Unternehmensnetzwerk per [1 VPN-Tunnel] erfolgen.

Für die elektronische Kommunikation dürfen nur genehmigte Unternehmens-Tools eingesetzt werden. Mit den Tools unseres Digital Me-Programms kannst Du problemlos mit Kollegen und Kunden auf der ganzen Welt kommunizieren und zusammenarbeiten.

Zu den Tools gehören u. a. SharePoint sowie eine Reihe von Cloud- bzw. Internet-basierten Anwendungen wie OneDrive, Yammer und Jabber. Weitere Anwendungen wie WIN10 und die zugehörigen Funktionen werden zentral durch Group IS bereitgestellt.

Alle anderen Cloud-Computing-Anwendungen, die nicht zentral von Group IS bereitgestellt werden, stellen keine genehmigten Unternehmens-Tools dar und dürfen deshalb im Rahmen der geschäftlichen Kommunikation nicht eingesetzt werden.



Das Internet hat zu unzähligen positiven Veränderungen in unserem Alltag geführt, aber es hat auch Nachteile, denn es öffnet Betrügern Tür und Tor, z. B. durch Phishing, Online-Viren, Trojanern usw. Es gibt jedoch eine Reihe von Maßnahmen zur Minderung des Risikos:

- Wenn Du unternehmenseigene Geräte nutzt, dann verwende stets die vom Unternehmen genehmigten Webbrowser
- Sei bei der Nutzung von Material aus dem Internet vorsichtig und denke insbesondere an urheberrechtliche Bestimmungen.
- Poste keine geschäftlichen Informationen im Internet, die für den internen Gebrauch bestimmt, vertraulich oder gar streng vertraulich sind.

In sozialen Online-Netzwerken verschwimmen die Trennlinien zwischen dem privaten, persönlichen und beruflichen Bereich. Einfach nur, indem Du Dich als Mitarbeiter von Computacenter zu erkennen gibst, erzeugst Du eine öffentliche Wahrnehmung. Vergewissere Dich deshalb, dass Deine Mitteilungen keine falschen Darstellungen enthalten oder unsere Bestimmungen zu Datenschutz und Verschwiegenheit verletzen.

Obwohl Social Media-Plattformen wie Facebook, LinkedIn, Xing großartige Tools sind, um sich zu vernetzen, können sie auch für sogenannte Aufklärungs(Reconnaissance)-Angriffe genutzt werden, bei dem Angreifer umfängliche Informationen sammeln. Zu viele Information preiszugeben, bietet Angreifern eine gute Ausgangslage und hilft ihnen, das benötige Material für einen Angriff auf Dich oder einen Deiner Mitarbeiter zu sammeln.

- Überprüfe Dein Profil auf detaillierte Angaben, und vermeide es, spezifische Produkt- oder Anbieternamen in Stellenbeschreibungen zu verwenden. Anstatt „Installation von Symantec Antivirus“ in eine Aufzählung aufzunehmen, könntest Du auch „Bereitstellung von Endgeräteschutz für 5.000 Server und Workstations“ schreiben.

- Vorsicht ist geboten bei neuen Kontakten, die Dich und Deine Kompetenz unmittelbar weiterempfehlen, insbesondere wenn Du noch nie mit ihnen zusammengearbeitet hast. Betrüger nutzen diese Taktik häufig, um schnell ein Vertrauensverhältnis aufzubauen.
- Verwende als Profilbild ein aktuelles Foto. Ein sorgfältig geführter Account mit einer Vielzahl von Kontakten, Gruppenmitgliedschaften und einem Foto macht es Betrügern schwerer, dein Profil zu fälschen.
- Überlege Dir sorgfältig, ob Du Verbindungsanfragen von ehemaligen Mitschülern annimmst. Oftmals richten Betrüger ihre Aufmerksamkeit auf die privaten Interessen von Mitarbeitern außerhalb der Arbeit, um den Anfangskontakt herzustellen.

Philip hat sich heute heftig über seine Vorgesetzte geärgert. Nun ist er zu Hause im Feierabend und nutzt wie gewohnt ein soziales Netzwerk. Er postet folgende Aussage unter seinem Profil:„Die neue Wettbewerbsstrategie, ab März die Rohstoffe zum Preis von 20,00 €/kg von der SchlagZu AG zu erwerben, halte ich für total bescheuert!“

Wie schätzt Du die Situation ein?

- ○ Sein Verhalten nach Feierabend ist ausschließlich Privatsache und geht das Unternehmen nichts an.
- ○ Der Austausch über soziale Netzwerke ist begrenzt und nicht öffentlich. Was dort gesagt wird, hat deswegen keine Auswirkungen auf das Unternehmen.
- ◉ Soziale Netzwerke lassen sich nicht effektiv eingrenzen und sind eine Form der Öffentlichkeit. Auch in diesem Rahmen ist Philip verpflichtet, die Geschäftsgeheimnisse und den Ruf des Unternehmens zu schützen.

Soziale Netzwerke sind öffentlicher Raum und damit keineswegs eine reine Privatsache. Philips Aussage kann der Wettbewerbsfähigkeit und dem Ruf des Unternehmens nachhaltig schaden. Achte deshalb bitte immer darauf, welche Auswirkungen eine unbedachte Nachricht haben könnte – denn für das Internet gibt es keinen Radiergummi.

Zusammenfassung

In dieser Lektion hast Du gelernt,…

- wie Du mit Risiken in der E-Mail-Kommunikation verantwortungsbewusst umgehest.
- welche Sicherheitsregeln Du bei der drahtlosen Datenübermittlung beachten musst.
- welche Unternehmens-Tools Du für die geschäftliche Kommunikation einsetzen solltest
- wie Du das Internet verantwortungsvoll nutzt
- dass soziale Netzwerke keine reine Privatsache sind.

Datenschutzverletzungen und Informationssicherheitsvorfälle:

Wenn du den Verdacht hast, auf einem Phishing-Versuch hereingefallen zu sein, weil Du auf einen Link geklickt oder einen Anhang geöffnet hast, oder bemerkt hast, dass sensible geschäftliche Informationen in einem sozialen Netzwerk gepostet wurden, melde bitte einen entsprechenden Informationssicherheitsvorfall über das NGSD.