

Die sieben Todsünden der digitalen Kommunikation

26.03.2018, 09:21 | IT, New Media & Software

Pressemitteilung von: *Brabblers*



Viele Unternehmen schützen ihre digitale Kommunikation nur unzureichend. (Quelle: margie/photocase)

München, 23. März 2018 - Die Brabblers AG beleuchtet die häufigsten Fehler von Unternehmen bei der digitalen Kommunikation.

Viele Unternehmen gehen zu sorglos mit ihrer digitalen Kommunikation um. Damit riskieren sie den Verlust von Betriebsgeheimnissen und laufen Gefahr, gegen gesetzliche Vorgaben wie die Datenschutzgrundverordnung (DSGVO) der Europäischen Union zu verstoßen. Das kann in beiden Fällen große Schäden verursachen und extrem teuer werden. Die Brabblers AG, Spezialist für sichere digitale Kommunikation, erläutert die sieben gängigsten Fehler.

1. E-Mails nicht verschlüsseln. Obwohl unverschlüsselte E-Mails die denkbar unsicherste Kommunikationsmethode darstellen, sind sie de facto immer noch Standard in deutschen Unternehmen. Cyber-Kriminellen ist damit Tür und Tor für die Vorbereitung und Durchführung ihrer Angriffe geöffnet. Unverschlüsselte E-Mails lassen sich relativ einfach belauschen und noch einfacher fälschen – etwa, um sich als Kollege oder Vorgesetzter auszugeben und den Empfänger so zur freiwilligen Preisgabe von Interna zu animieren.
2. Empfängerkreis unnötig aufblähen. Zunächst schickt einfach nur ein Mitarbeiter einem anderen eine E-Mail. Im Laufe der weiteren Korrespondenz wächst der Empfängerkreis dann ständig an. Kollegen, Partner und Kunden werden massenweise hinzugefügt – das Thema könnte sie ja schließlich auch interessieren. So gelangen am Ende Informationen an Personen, für die sie ursprünglich nie gedacht waren. Und wenn dabei noch die Mail-Adressen ins für alle sichtbare CC-Feld eingegeben werden, kommt häufig auch noch ein Verstoß gegen den Schutz personenbezogener Daten hinzu.
3. WhatsApp und Co. nutzen. Auch die Nutzung von Kommunikationsdiensten wie WhatsApp ist aus rechtlicher Sicht äußerst problematisch. So liest WhatsApp die Adressbücher der Mitarbeiter aus und gibt die Daten an die Konzernmutter Facebook weiter – eine klare Verletzung der DSGVO. Andere Lösungen wie Slack, Hipchat oder der Facebook Messenger stehen hier auch nicht viel besser da. Zudem werden die Daten dieser Tools meist in den USA gespeichert und damit in einem Land, dessen allgemeines Datenschutzniveau mutmaßlich zu niedrig für die Erfüllung der DSGVO

ist.

4. Dokumente über Public Clouds austauschen. Der Austausch von Dokumenten über Cloud-Dienste wie Google Drive, Dropbox oder Skype birgt ebenfalls große Risiken. Derartige Dienste verschlüsseln ihre Dateien meist nur unzureichend und machen sensible Tabellen oder Präsentationen damit auslesbar. Zum einen für die Anbieter selbst, aber auch Hackern wird die Arbeit damit deutlich erleichtert. Da diese Dienste ihre Daten ebenfalls meist in den USA speichern, sind sie außerdem den Zugriffen neugieriger US-Behörden ausgeliefert und häufig nicht DSGVO-konform.

5. Arbeit nach Hause schicken. Eine andere gängige Praxis in vielen Unternehmen verursacht ähnliche Probleme. Um eine Präsentation oder ein Angebot am Abend oder am Wochenende nochmal in aller Ruhe daheim zu überarbeiten, schicken Mitarbeiter sie sich an ihre privaten E-Mail-Adressen. Auch dort liegen die Dokumente dann häufig nicht ausreichend gesichert auf den Servern der Anbieter, die ebenfalls nicht selten ihren Sitz in den USA haben.

6. Speichermedien nicht schützen. Nicht nur bei der Übertragung und Speicherung der Kommunikationsdaten auf den Servern der Anbieter, sondern auch auf den Endgeräten liegt oft einiges im Argen. So werden die Daten in den lokalen Speichern von Smartphones, Tablets oder Desktop-PCs meist unverschlüsselt vorgehalten. Damit sind sie im Fall eines erfolgreichen Cyber-Angriffs ungeschützt; wird einem Mitarbeiter ein Mobilgerät gestohlen oder verliert er es, kann auch der Dieb oder Finder die Daten unter Umständen auslesen.

7. Passwortsicherheit vernachlässigen. Last but not least gehen Mitarbeiter meist immer noch zu lax mit den Passwörtern für ihre Kommunikationsdienste um. Sie verwenden Namen oder kurze Begriffe statt ausreichend lange und komplexe Zeichenfolgen. Das macht es Hackern sehr einfach, die Passwörter zu knacken. Nutzen Mitarbeiter komplexe Zeichenfolgen, können sie sich diese natürlich meist nicht auswendig merken und müssen sie deshalb irgendwo abspeichern. Das tun sie allerdings dann meist völlig ungeschützt irgendwo auf ihrem Rechner – wenn sie sie nicht gleich auf einem Post-it notieren und an ihren Bildschirm kleben.

„Unternehmen müssen ihre Mitarbeiter für einen sicheren und verantwortungsbewussten Umgang mit Kommunikationsdaten sensibilisieren. ‚Katze123‘ ist einfach nicht das beste Passwort“, sagt Daniel Eyring, Team Lead Engineering bei Brabbl. „Viele Gefahren können Unternehmen aber auch durch den Einsatz einer geeigneten Kommunikationslösung ausschließen. Sie sollten auf ein System setzen, das alle übertragenen und ruhenden Daten vollverschlüsselt – und zwar so, dass selbst der Anbieter des Systems sie nicht auslesen kann. Außerdem sollten sie europäischen Anbietern vertrauen, denn nur sie können DSGVO-Compliance sicherstellen und die Daten vor US-amerikanischen Behörden schützen.“

Portrait

Über Brabbl

Das Münchner Startup Brabbl AG entwickelt unter dem Namen „ginlo“ eine Kommunikationsplattform, die Privatsphäre für Privatpersonen und Vertraulichkeit für Unternehmen sicherstellt.

Unternehmen steht eine Ende-zu-Ende verschlüsselte und administrierbare IT-Lösung für die Kommunikation ihrer Mitarbeiter zur Verfügung. Sie wird ausschließlich in Deutschland gehostet. Der Zugriff auf sämtliche Inhalte ist allein den Unternehmen beziehungsweise deren Nutzern möglich. Damit ist gewährleistet, dass die Mitarbeiter zu 100 Prozent vertraulich und effizient kommunizieren und Daten austauschen können.

Brabblers wurde 2015 von den GMX Gründern Karsten Schramm, Peter Köhnkow und Eric Dolatre gemeinsam mit Jörg Sellmann ins Leben gerufen. Weitere Informationen: www.brabblers.ag und www.ginlo.net.

News-ID: 997807 • Views: 579 (Stand: 07.08.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/997807/Die-sieben-Todsunden-der-digitalen-Kommunikation.html>