Mit der GM-Methode sicher im Home-Office

Immer mehr Unternehmen bieten Ihren Mitarbeitern die Möglichkeit, von zuhause aus zu arbeiten. Dies schafft mehr Flexibilität, bringt jedoch auch *Herausforderungen* mit sich. Bei der *GM-Methode* handelt es sich um den *GESUNDEN MENSCHENVERSTAND*. Mittels dieser *Methode* kombiniert mit den folgenden 5 Tipps, leisten Sie Ihren Beitrag, sicher von zuhause aus zu arbeiten. Das tolle daran ist, dass nicht nur Ihr Unternehmen sondern auch *Sie selbst und Ihre Familie* davon provitieren, wenn Sie ein cybersicheres Zuhause schaffen.

Sie sind die „First Line of Defense“

Technologie alleine kann Sie nicht vollständig vor Cyber-Angriffen schützen – *SIE* selbst sind die beste Verteidigung. Cyber-Angreifer wissen, dass es einfacher ist, *Sie* anstatt Ihrer Computer und adere Geräte anzugreifen, um an das gewünschte Ziel zu gelangen. Cyber-Angreifer nutzen bspw. Stress-Situationen gezielt aus, um ihre Opfer zu Handlungen zu überreden, zu denen sie sich sonst nicht einfach verleiten lassen würden. Cyber-Kriminelle versuchen mit verschiedenen Tricks per Telefon oder eMail, an Ihre Daten oder Ihr Passwort zu gelangen. Sie schlüpfen in die Rolle anderer, eigenen sich den Firmenjargon an um möglichst glaubhaft zu wirken bzw. erzeugen künstlich herbeigeführte Probleme und bieten anschließend Hilfestellung an.

Sofern möglich, halten Sie sich also auch zuhause an dieselben Sicherheitsrichtlinien, wie sie im Unternehmen gelten. Melden Sie Informationssicherheits- und Datenschutzvorfälle ggf. unverzüglich an die zuständigen Stellen.

Indikatoren für Social Engineering Angriffe sind:

Jemand versucht Sie zu einer Handlung zu bewegen indem Dringlichkeit durch Angst, Einschüchterung, eine Krise oder einen wichtigen Termin erzeugt wird. *Kommen Sie in ungewöhnlichen Situationen nicht immer sofort jeder Aufforderung nach. Notieren Sie sich bei Telefonanrufen die Nummer und bieten einen sofortigen Rückruf an.*	Sie erhalten unaufgefordert eine eMail mit dem Ziel, dass Sie auf einen Link klicken, einen Anhang öffnen oder Ihre persönlichen Daten bzw. Zugangsdaten prüfen bzw. eingeben sollten. *Ignorieren Sie solche eMails und fragen Sie bei Unsicherheit am besten über einen alternativen Weg beim Absender nach.*	Ein freundlicher Support Mitarbeiter kontaktiert Sie, um wichtige Wartungs- oder Installationsarbeiten durchzuführen und bittet Sie um Ihr Passwort bzw. ein Programm zu installieren, damit der Support remote erledigt werden kann. *Kommen Sie in solchen Fällen den Aufforderungen auf keinen Fall nach und wenden sich umgehend an Ihre IT-Abteilung und melden den Fall.*

Das Heim-Netzwerk

Vermutlich verfügen auch Sie in Ihrem Haushalt über einen WLAN-fähigen Internet-Router. Damit sich Ihre Geräte verbinden können, senden diese Router ständig ein WLAN-Signal aus. Dies hat zur Folge, dass in den meisten Fällen 24 Stunden am Tag eine Verbindung in Ihr WLAN-Netz möglich ist – leider meist auch über die eigenen vier Wände hinaus.

Dadurch ist es besonders wichtig, WLAN-Netzwerke gut abzusichern.

Je nachdem, wie der Fernzugang ins Unternehmens-Netzwerk eingerichtet wurde, sollten Sie nach Möglichkeit den Web-Browser und eMail-Client in der jeweiligen Remote-Verbindung nutzen, da	Sie sollten darauf achten, dass sich nur vertrauenswürdige Personen mit Ihrem Netzwerk verbinden. Erstellen Sie zum Schutz vor fremden Zugriffen auf Ihr WLAN-Netzwerk komplexe WLAN-Schlüssel. Die meisten	Ändern Sie immer das Standard-Passwort Ihrer Netzwerk-Geräte und verwenden Sie nicht das Administrator-Passworts Ihres WLAN-Routers als WLAN-Schlüssel.

dadurch die Schutz-Systeme Ihrer Organisation greifen.	WLAN-Router unterstützen bereits Optionen für die Einrichtung eines Gäste-WLANs und zur Isolierung verbundener Geräte. *Wenn Sie Unterstützung benötigen, steht Ihnen unter Umstände Ihr Internet-Anbieter zur Verfügung.*	

Passwörter

Schwache Passwörter sind die Achillesferse der Informationssicherheit eines Unternehmens. In vielen Fällen können Angreifer Passwörter entweder selbst erraten, oder es werden einfache Programme benutzt, die häufig genutzte Passwörter durchtesten, bis das passende gefunden wurde. Oft schon führen schlecht gewählte Passwörter dazu, dass ganze Unternehmen kompromittiert wurden. Daher ist es besonders wichtig, starke Passwörter zu wählen. Am besten denkt man bei der Vergabe des Passworts an eine Zahnbürste:

- man sollte eine gute wählen
- man sollte sie regelmäßig wechseln
- man sollte sie mit niemanden teilen

Achten Sie also bei der Wahl des Passworts besonders darauf, dass

- *NIEMALS* das *gleiche* Passwort über mehrere Systeme verwendet wird
- man zur Notierung von Passwörtern geeignete Tools *wie Passwort-Manager* nutzt
- "Allerwelts-Passwörter" und Kombinationen wie 123456, QWERTZ, ASDFG, usw. gemieden werden
- Name von Haustieren, Verwandten, Kinder usw. sowie Geburtsdatum *NICHT* verwendet werden
- *KEINE* Passwörter gewählt werden, die in Wörterbüchern vorkommen

- je nach Firmenrichtlinie mindestens 12 Zeichen aus Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen verwendet werden
  (vor allem aber spielt die Länge des Passworts eine Rolle - *JE LÄNGER, DESTO BESSER!)*
- das Passwort *NICHT* weitergegeben wird und auch *KEINE* Informationen, wie sich das Passwort zusammensetzt, geteilt werden
- die Passwörter laut Firmenrichtlinie regelmäßig bzw. *bei Kompromittierung SOFORT* geändert werden

---

Updates

Sie sollten sicherstellen, dass Ihre Computer, mobilen Geräte, Programme und Apps auf dem aktuellen Stand gehalten werden. Cyber-Kriminelle versuchen ständig, Schwachstellen in Systemen zu finden und auszunutzen. Werden Geräte, Programme und Apps regelmäßig mit Updates versorgt, wird es für Kriminelle bedeutend schwerer, Sie auf diese Art anzugreifen. Aktivieren Sie wenn möglich automatische Updates, damit diese auf Ihren Geräten von selbst eingespielt werden. Diese Regel ist nicht nur auf Unternehmens-Geräte anzuwenden, sondern auf sämtliche Technologien, die sich ins Internet verbinden. Smart-TVs, Überwachungs-Kameras, Spiele-Konsolen, internetfähige Baby-Phone, Heizungs-Steuerung usw.

Kinder und Gäste

Gleich wie im Unternehmen ist sicherzustellen, dass keine fremde Personen die Systeme, mit denen auf Firmendaten zugegriffen werden, nutzen. Im Home-Office betrifft das vor allem Familienmitglieder, Kinder und Gäste. Ihnen muss verständlich gemacht werden, dass Firmengeräte nicht benutzt werden dürfen, da versehentlich Daten gelöscht oder modifiziert bzw. Geräte infiziert werden könnten. Unter Umstände würde dies schwere Informationssicherheits- bzw. Datenschutz-Folgen mit sich bringen.
