IT-SECURITY IM HOMEOFFICE: EINE ORIENTIERUNGSHILFE VON NETZLINK

INHALT

EINLEITUNG

Vielleicht kommt Ihnen folgendes Szenario bekannt vor: Sie erhalten eine E-Mail von der Adresse Ihres Vorgesetzten. Darin die Aufforderung, eine Zahlung auszuführen. Sie wundern sich, denn Ihr Chef hat diese Zahlung noch nie vorher erwähnt. Wären Sie jetzt vor Ort im Unternehmen, könnten Sie einfach in sein Büro gehen und persönlich nachfragen. Die Herausforderung: Sie sind nicht im Büro, sondern im Homeoffice. Natürlich könnten Sie Ihren Chef anrufen oder ihn per Nachricht fragen, was es mit dieser Zahlung auf sich hat. Aber Sie wissen, dass er heute wieder sehr viel zu tun hat und eigentlich wollen Sie ihn ja bestmöglich unterstützen. Am besten, so denken Sie, überweisen das Geld einfach und die Sache ist erledigt...

Cyberangriffe passieren jeden Tag. Phishing-Mails, wie in diesem fiktiven Szenario, bei denen Angreifer im Namen von Vorgesetzten oder Mitarbeitenden Zahlungsaufforderungen schicken oder nach vertraulichen Daten fragen, sind nur ein mögliches Beispiel. Seit viele Arbeitnehmende vermehrt im Homeoffice sind, ist die Zahl der Angriffe auf Unternehmen deutlich gestiegen. Umso wichtiger ist es, den wachsenden Bedrohungen eine umfassende IT-Security-Strategie entgegenzusetzen. Dieses Booklet gibt einen Überblick über IT-Sicherheitsrisiken und Maßnahmen für die Arbeit im Homeoffice.

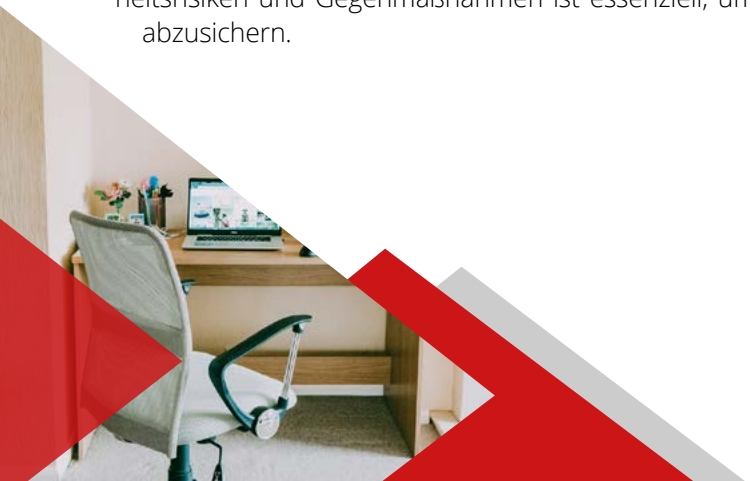
Für alle Fragen steht das Netzlink-Expertenteam wie gewohnt zur Verfügung. Gemeinsam erarbeiten wir mit Ihnen eine IT-Security-Strategie!

ZUR BEDEUTUNG VON IT-SECURITY IM HOMEOFFICE

Ob Arbeitnehmende im Büro oder im Homeoffice sind - die Bedeutung von IT-Security ist gleichbleibend hoch. IT-Sicherheitsmaßnahmen für das Homeoffice sind nicht grundlegend anders als die Maßnahmen bei Büroarbeit, jedoch verändert sich die Art und Intensität der Umsetzung. Im besten Fall durchdringt IT-Security ein Unternehmen ganzheitlich. Das bedeutet, dass Hardware und Software abgesichert sind und das Thema in den Köpfen aller Mitarbeitenden einen hohen Stellenwert hat – immer und überall.

Die Realität sieht im Homeoffice jedoch meist anders aus: Werden im Büro noch gemeinsam mit Kollegen und Kolleginnen Sicherheitsrichtlinien verfolgt, birgt das Homeoffice die Gefahr, dass die Bemühungen vernachlässigt werden. Wenn der Küchentisch zum Arbeitsplatz wird und die Grenzen zwischen Arbeits- und Privatleben verschwimmen, gerät das Bewusstsein für unternehmensrelevante IT-Security-Risiken und -Maßnahmen meist in den Hintergrund. Die Versuchung steigt, ein berufliches Dokument offen liegen zu lassen oder den Dienstlaptop für den privaten Serienmarathon nach Feierabend zu nutzen – und damit steigen auch die Einfallstore für Cyberangriffe.

Generell gilt: Bestehen etablierte Security-Richtlinien im Unternehmen, beherzigen Mitarbeitende diese mit höherer Wahrscheinlichkeit sowohl im Büro als auch im Homeoffice. Das A und O für IT-Security ist dabei die Awareness jeder einzelnen Person. Über 80 Prozent der weltweiten Sicherheitsvorfälle sind dem „Faktor Mensch“ geschuldet. Die Kenntnis der Mitarbeitenden über Sicherheitsrisiken und Gegenmaßnahmen ist essenziell, um die Arbeit im Homeoffice abzusichern.



WAS PASSIERT EIGENTLICH BEI EINEM CYBERANGRIFF?

IT-Security ist wichtig, klar. Doch was genau bei einem Cyberangriff passiert und welche negativen Folgen dieser haben kann, ist für den einzelnen Mitarbeitenden im Unternehmen eventuell nicht so eindeutig. Wir glauben: Wer die Hintergründe versteht ist eher gewillt, seinen Beitrag für die Sicherheit zu leisten – auch eigenverantwortlich im Homeoffice.

Was passieren kann, wenn Sie zum Beispiel auf einen manipulierten Download-Link geklickt und sich Schadsoftware „einfangen“ haben, oder Angreifer durch ein Datenleck Zugriff erlangen, haben wir anhand von Beispielen zusammengetragen:

- **Ransomware:** Diese Schadsoftware verschlüsselt alle Dateien auf Ihrem PC und im schlimmsten Fall im gesamten Unternehmensnetzwerk. In vielen Fällen fordern die Angreifer Lösegeld, damit sie diese wieder „freigeben“.
- **Spyware:** Mit diesem ungebetenen Gast auf Ihrem Gerät werden Ihre Aktivitäten überwacht und alle Tastenanschläge mitgelesen. Auf diese Weise können Angreifer nicht nur an Passwörter, sondern auch an sämtliche andere vertrauliche Daten gelangen.
- **RAT (Remote Access Trojaner):** Mit dieser Schadsoftware wird ein Trojaner, eine Hintertür, auf Ihrem System installiert, durch die Unbefugte von außen Zugriff auf den eigenen Rechner erlangen. Dass dies teilweise lange Zeit oder auch nie bemerkt wird, macht es umso gefährlicher.

SICHERHEITSRISIKEN IM HOMEOFFICE

Generell können Cyberangriffe durch die Manipulation von Menschen oder durch ausgenutzte Schwachstellen in Hard- oder Software erfolgreich sein. Speziell im Homeoffice gibt es eine Vielzahl möglicher Einfallstore.

- **Phishing-Mails:** Besonders im Homeoffice besteht die Gefahr, einem Angriff per Phishing-Mail zum Opfer zu fallen. Wird die Arbeit in Isolation erledigt und Kolleginnen und Kollegen sind nicht direkt erreichbar, steigt die Hemmschwelle, bei E-Mails mit ungewöhnlichen Aufforderungen (oder Aussehen) nachzufragen.
- **Privater Router:** Arbeiten die Mitarbeitenden im Büro, kommunizieren sie größtenteils über das abgesicherte Unternehmensnetzwerk. Im Homeoffice nutzt jeder Mitarbeitende einen eigenen Router, der potenziell verwundbar sein kann. Dadurch eröffnen sich neue Angriffsvektoren und die Gefahr von Schwachstellen steigt enorm.
- **Vermischung von Gerätenutzung für Beruf und Privates:** Durch private Nutzung von Firmengeräten oder Nutzung von Privatgeräten für die Arbeit kann schadhafte Software auf Privatgeräten Zugriff auf das firmeninterne Netzwerk erlangen. Dies gilt sowohl für Laptop und Smartphone, aber auch beispielsweise ein USB-Stick kann infiziert sein.
- **Schatten-IT:** Private Anwendungen auf dem Dienstgerät, von denen die IT-Abteilung nichts weiß und die sie entsprechend nicht absichern kann, wird schnell zu einem Sicherheitsrisiko.
- **Datenschutz:** Genau wie im Büro besteht im Homeoffice die Gefahr, dass vertrauliche Informationen Dritten zugänglich werden. In den eigenen vier Wänden birgt die fehlende Abgrenzung von Arbeits -und Privatleben das Risiko, dass Informationen in die Hände von Mitbewohnern, Besuchern oder gänzlich Fremden gelangen.

SICHERHEITSMAßNAHMEN IM HOMEOFFICE

Die Einfallstore für Sicherheitsvorfälle gilt es abzusichern. Durch aufmerksames Verhalten und gezielte Maßnahmen kann IT-Security im Homeoffice gewährleistet werden.

UNTERNEHEMSÜBERGREIFENDE MAßNAHMEN

- **Firmeneigene Geräte:** Im Optimalfall arbeiten Mitarbeitende im Homeoffice mit Firmengeräten, die über Firewall und Malware-Scanner verfügen.
- **Updaterichtlinien:** Hardware und Software auf den Geräten der Mitarbeitenden sollten auf dem neuesten Stand sein. Am besten werden Updates per Richtlinien automatisch gesteuert.
- **Verschlüsselung:** Unabdingbar, um die Sicherheit aufrecht zu erhalten, ist die Authentifizierung der Mitarbeitenden vor dem Zugriff auf Endgeräte und Firmendaten durch Login per Passwort. Äußerst sinnvoll ist eine Zwei-Faktor-Authentifizierung, zum Beispiel per App oder Hardware-Token.
- **VPN:** Um das Unternehmensnetzwerk vor unberechtigtem Zugriff abzusichern, sollte der Zugang nur per VPN möglich sein.

MAßNAHMEN DER MITARBEITENDEN

- **Nutzung von Firmengeräten:** Arbeiten Sie, wenn möglich, mit firmeneigenen Geräten. Verwenden Sie diese ausschließlich für berufliche Zwecke und vermeiden Sie die private Nutzung. Speichern Sie keine firmeninternen Informationen auf privaten Geräten.
- **Absicherung des eigenen Netzwerks:** Schützen Sie Ihren eigenen Router mit einem sicheren Passwort und WPA2-Verschlüsselung. Zudem empfiehlt es sich, ein eigenes WLAN-Netz für Arbeitsgeräte einzurichten.
- **Datenspeicherung:** Speichern Sie Ihre Daten nicht lokal, z. B. auf dem Desktop, sondern auf einer passwortgeschützten Umgebung wie einem File-Server.
- **Passwortmanagement:** Verwalten Sie Ihre Passwörter nicht lokal und schreiben Sie sich diese auch nicht anderweitig auf. Sinnvoll zur Organisation von Passwörtern ist ein Passwort-Manager-Programm.
- **Gerätesperrung:** Sperren Sie Ihr Endgerät immer, wenn Sie es nicht verwenden. Niemand anderes außer Sie sollte Zugriff darauf haben.
- **Verschluss von Unterlagen:** Schützen Sie Unterlagen vor den Augen Dritter. Lassen Sie nichts offen herumliegen und schließen Sie Ihre Materialien ein. Papierdokumente sollten geschreddert und nicht im Originalzustand im Hausmüll entsorgt werden.
- **Videohintergrund:** Ein Poster mit dem Projektzeitplan oder wichtige Notizen an der Pinnwand sollten zwar für Sie sichtbar sein, jedoch nicht für Kunden oder Auftraggeber. Achten Sie darauf, dass keine firmeninternen Informationen im Hintergrund bei einer Videokonferenz erkennbar sind.

Und das Wichtigste ist: Bleiben Sie aufmerksam und fragen Sie im Zweifelsfall nach!

FAZIT: IT-SECURITY TRIFFT ARBEITSREALITÄT

Die Sicherheitsmaßnahmen, die wir Ihnen in diesem Booklet an die Hand geben, mögen vielleicht auf den ersten Blick Unbehagen bei Ihnen auslösen oder fern ab von Ihrer Arbeitsrealität im Homeoffice erscheinen. Schließlich hat nicht jeder ein abgetrenntes Arbeitszimmer zur Verfügung, um Geräte und Unterlagen vor Dritten abzuschirmen. Auch die Angst, im Fall eines Phishing-Angriffs im Homeoffice auf sich allein gestellt zu sein und sich unbedacht zu verhalten, kann groß sein.

Wir möchten Sie ermutigen, Sicherheitsmaßnahmen in Ihrer Arbeitsrealität im Homeoffice so gut wie möglich umzusetzen. In diesem Fall gilt: Wichtiger als perfektes Verhalten ist Ihr eigenes Bewusstsein für die Thematik. Das bedeutet, dass Sie Ihrer Arbeit im Homeoffice mit offenen Augen nachgehen. Fragen Sie aktiv nach, wenn Ihnen eine Mail seltsam vorkommt und Sie sich nicht sicher sind, ob Sie dem Absender vertrauen können. Überprüfen Sie regelmäßig, ob Geräte und Software auf dem neusten Stand und Ihre Passwörter sicher sind. Und wenn doch einmal etwas passiert und Sie zum Beispiel versehentlich auf einen Link in einer Phishing-Mail geklickt haben, melden Sie sich umgehend bei Ihrer internen IT-Abteilung. Diese kann den Angriff identifizieren und entsprechende Maßnahmen einleiten. Machen Sie sich jederzeit bewusst, dass Sie dazu beitragen können, Ihr Unternehmen zu schützen.

Und wenn gar nichts mehr geht, gibt es immer noch uns – wir helfen Ihnen in jeder Security-Situation!

BESUCHEN SIE UNS

www.netzlink.com

Social Media

de.linkedin.com/company/netzlink-informationstechnik-gmbh

xing.com/pages/netzlinkinformationstechnikgmbh

twitter.com/netzlink

www.facebook.com/netzlink

IMPRESSUM

Herausgeber:
Netzlink Informationstechnik GmbH
IT-Campus Westbahnhof
Westbahnhof 11
38118 Braunschweig
Telefon: (+49) 0531 707 34 30

Redaktion:
Netzlink Informationstechnik GmbH

Gestaltung:
Netzlink Informationstechnik GmbH

Fotos:
pexels.com

Version:
1.0 // 29. April 2021