Aktueller Hinweis

Tipps für sicheres mobiles Arbeiten

Hinweis: Mit Telearbeit sind hier alle Arbeiten von zu Hause aus oder unterwegs gemeint.

1. Regelungen für Telearbeiter / Sicherheitsrichtlinie für die Telearbeit

Ist die Telearbeit in einer Institution nicht oder nur unzureichend geregelt, entstehen verschiedene Risiken, insbesondere – aber nicht ausschließlich – im Hinblick auf die Informationssicherheit. Der Abfluss von Informationen stellt dabei nur eines von zahlreichen Bedrohungsszenarien dar. Daher muss für alle Telearbeiten geregelt werden, welche Informationen (sowohl auf Papier, aber auch in IT-Systemen) außerhalb der Institution transportiert und bearbeitet werden dürfen, wer diese mitnehmen darf und welche Schutzvorkehrungen (Sicherheitsmaßnahmen) dabei zu treffen sind.

Es sollte auch klar geregelt werden, welche Kommunikationsmöglichkeiten bei der Telearbeit unter welchen Rahmenbedingungen genutzt werden dürfen.

Alle relevanten Sicherheitsmaßnahmen der Telearbeit müssen in einer für die Telearbeiter verpflichtenden Sicherheitsrichtlinie dokumentiert werden.

2. Sensibilisierung der Telearbeiter

Häufig gibt es in Institutionen zwar organisatorische Regelungen und technische Sicherheitsmaßnahmen zum Schutz der Informationen. Diese werden jedoch durch einen sorglosen Umgang mit den Vorgaben und der Technik oft wieder ausgehebelt. Daher müssen die Telearbeiter anhand der Sicherheitsrichtlinie für die Telearbeit oder eines dafür vorgesehenen Merkblatts für die Gefahren, die mit der Telearbeit verbunden sind, sensibilisiert werden. Sie müssen die Gefahren kennen, die beispielsweise durch den unangemessenen Umgang mit Informationen, die unsachgemäße Vernichtung von Daten und Datenträgern, durch einen unsachgemäßen Transport von Arbeitsmaterial oder durch eine unsichere Kommunikation entstehen können. Außerdem müssen sie für den Wert der Ihnen anvertrauten Informationen sensibilisiert werden. Sie müssen in die entsprechenden Sicherheitsmaßnahmen der Institution eingewiesen und im Umgang mit diesen geschult werden.

3. Zutritts- und Zugriffsschutz

Bei einem Telearbeitsplatz kann nicht die gleiche infrastrukturelle Sicherheit vorausge-

setzt werden, wie sie in den Büroräumen einer Institution anzutreffen ist. So ist z. B. der häusliche Arbeitsplatz oft auch für Besucher oder Familienangehörige zugänglich. Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist. Den Telearbeitern muss bekannt gegeben werden, welche Regelungen und Maßnahmen zum Einbruch- und Zutrittsschutz am Telearbeitsplatz zu beachten sind. So muss beispielsweise darauf hingewiesen werden, Fenster zu schließen und Türen abzuschließen, wenn der Telearbeitsplatz nicht besetzt ist, etwa in einem Hotelzimmer. Generell muss sichergestellt werden, dass Unbefugte zu keiner Zeit auf dienstliche IT und Unterlagen zugreifen können. Am häuslichen Arbeitsplatz müssen hierfür ausreichende verschließbare Behältnisse wie ein abschließbarer Schreibtisch, Rollcontainer oder Schrank vorhanden sein. Jeder Mitarbeiter muss seinen häuslichen Arbeitsplatz aufgeräumt hinterlassen und sicherstellen, dass keine sensitiven Informationen frei zugänglich sind.

4. Sicherheitstechnische Anforderungen an die für die Telearbeit eingesetzten IT-Systeme / Härtung der eingesetzten IT-Systeme

Sind die für die Telearbeit eingesetzte IT-Systeme beispielsweise unsicher konfiguriert, können Sicherheitsprobleme entstehen, z. B. der Verlust der Vertraulichkeit durch unbefugten Zugriff.

Zur Minimierung der Angriffsfläche sollten die für die Telearbeit verwendeten IT-Systeme gehärtet sein. Ferner sind Standardmaßnahmen zum Schutz von IT-Systemen umzusetzen – hierzu zählen insbesondere das Einspielen aktueller Software-Patches und AV-Signaturen sowie der Einsatz einer Firewall. Alle Zugangsmöglichkeiten auf die Server der Institution sowie alle Zugriffsrechte auf die darauf gespeicherten Informationen müssen auf das notwendige Mindestmaß beschränkt sein.

Sollten die Mitarbeiter bei der Arbeit im Home-Office auf private Laptops zurückgreifen müssen, muss beachtet werden, dass viele dieser genannten Maßnahmen nur in Eigenverantwortung durch die Nutzer umgesetzt werden können. Daher empfiehlt sich (neben der Risikoabwägung) eine zusätzliche Sensibilisierung der Mitarbeiter, um Bedrohungen zu minimieren.

5. Verschlüsselung von tragbaren IT-Systemen und Datenträgern

Am Telearbeitsplatz können Angreifer häufig einfacher auf vertrauliche Informationen zugreifen, die sich auf fest eingebauten und austauschbaren Speichermedien, aber auch auf Papier befinden. Werden Informationen unberechtigt gelesen oder preisgegeben, hat das jedoch schwerwiegende Folgen für die gesamte Institution. Unter anderem kann es zu Wettbewerbsnachteilen und finanziellen Schäden kommen. Sogar Gesetzesverstöße sind möglich. Zusätzlich ist der mobile Arbeitsplatz meist nicht so gut abgesichert wie der Arbeitsplatz in einem Unternehmen oder in einer Behörde. Dienstliche IT-Geräte und Dokumente können daher z. B. während einer Bahnfahrt, aus einem Hotelzimmer oder aus externen Konferenzräumen leichter gestohlen werden. Daher sollten tragbare IT-Systeme und Datenträger unbedingt verschlüsselt werden.

6. Nutzung von Bildschirmschutzfolien

Gerade bei der Arbeit in öffentlichen Umgebungen wie z. B. Bahn oder Flugzeug, besteht die Gefahr des „über die Schulter schauen“ (Shoulder Surfing). So können vertrauliche Informationen wie z. B. Kundendaten oder Passwörter unberechtigten Dritten bekannt werden. Auch videoüberwachte Bereiche können ein Sicherheitsproblem darstellen, da hochauflösende Kameras alle Eingaben und den Inhalt des Bildschirms aufzeichnen können. Daher sollten Maßnahmen wie Bildschirmschutzfolien genutzt werden, die die Einsichtnahme von der Seite verhindern. Da dies nicht vor allen Gefahren schützt, muss grundsätzlich abgewogen werden, welche

Tätigkeiten an öffentlichen Orten durchgeführt werden können und welche nicht.

7. Sicherer Remote-Zugriff auf das Netz der Institution

Um dienstliche Aufgaben erledigen zu können, müssen Telearbeiter auf interne Ressourcen der Institution zugreifen. Werden hierfür unsichere Protokolle verwendet, können Informationen abgehört oder manipuliert werden. Um Telearbeitern einen sicheren Fernzugriff auf das Netz der Institution zu ermöglichen, muss daher zuvor von der Institution ein sicherer Remote-Zugang eingerichtet worden sein, z. B. kryptografisch abgesicherte Virtual Private Networks (VPN).

Über öffentlich zugängliche Netze dürfen die Mitarbeiter nur über einen sicheren Kommunikationskanal (z. B. kryptografisch abgesicherte VPN) auf interne Ressourcen der Institution zugreifen. Dieser Zugriff muss auf vertrauenswürdige IT-Systeme und Benutzer sowie auf die benötigten Benutzungszeiten beschränkt werden

8. Datensicherung

Bei mobilen IT-Systemen ist die Gefahr der Zerstörung durch Stürze, Schäden durch Transport, ungünstige klimatischen Bedingungen sowie falsche Aufbewahrung wesentlich größer, als wenn ein stationärer Arbeitsplatz genutzt wird. Auch ein Verlust durch Diebstahl oder einfaches „Liegen lassen“ kommt häufig vor. Daher sollte eine regelmäßige Datensicherung der lokal gespeicherten Daten durchgeführt werden. Idealerweise werden wichtige Daten überhaupt nicht lokal gespeichert. Falls dies auf externen Medien erfolgt, sollte sinnvollerweise jeweils eine Generation der Datensicherungen in der Institution hinterlegt werden.

9. Zeitnahe Verlustmeldung

Wenn der Fall eintritt, dass mobile Geräte abhandengekommen sind, ist eine zeitnahe Verlustmeldung notwendig. So kann die Institution zeitnah mit Maßnahmen wie das Ändern von Passwörtern oder das Sperren von Zugängen reagieren. Hierfür muss es klare Meldewege und Ansprechpartner innerhalb der Institution geben, die den Mitarbeitern bekannt sind.

10. Support für Telearbeitsplätze

Damit die Telearbeiter einsatzfähig bleiben, sollte für sie Ansprechpartner für Hard- und Softwareprobleme benannt werden.

11. Arbeiten mit fremden IT-Systemen/Netzen

Die Institution muss regeln, wie Mitarbeiter mit institutionsfremden IT-Systemen/Netzen arbeiten dürfen. Da sich das Schutzniveau solcher IT-Systeme /Netzen von dem der eigenen Institution stark unterscheiden kann, muss jeder Telearbeiter über die Gefahren fremder IT-Systeme/Netze aufgeklärt werden.

12. Entsorgung von vertraulichen Informationen

Ist es Mitarbeitern am Telearbeitsplatz nicht möglich Informationen (z. B. Datenträger und Dokumente) in geeigneter Weise zu entsorgen, kann es passieren, dass sie einfach in den Hausmüll geworfen werden oder unterwegs unsachgemäß entsorgt werden. Angreifer können daraus jedoch wertvolle Informationen gewinnen, die sich gezielt für Erpressungsversuche oder zur Wirtschaftsspionage missbrauchen lassen. Die Folgen reichen vom Wissensverlust bis zur Existenzgefährdung der Institution, z. B. wenn dadurch wichtige Aufträge nicht zustande kommen oder Partnerschaften scheitern.

Vertrauliche Informationen sollten auch zu Hause oder unterwegs sicher entsorgt werden. Bevor ausgediente oder defekte Datenträger und Dokumente weggeworfen werden, muss überprüft werden, ob sie sensible Informationen enthalten. Ist dies der Fall, müssen die Datenträger und Dokumente wieder mit zurücktransportiert werden und auf institutionseigenem Wege entsorgt bzw. vernichtet werden

13. Umgang mit dienstlichen Unterlagen bei erhöhtem Schutzbedarf am Telearbeitsplatz

Wenn Mitarbeiter dienstliche Unterlagen oder Informationen mit erhöhtem Schutzbedarf bearbeiten müssen, sollte überlegt werden, von einem Arbeitsplatz außerhalb der Institution ganz abzusehen. Anderenfalls sollte der Telearbeitsplatz durch erweiterte, hochwertige technische Sicherungsmaßnahmen geschützt werden.

14. Eindeutige Verifizierung.

Sorgen Sie für eindeutige Kontaktstellen und Kommunikationswege, die von den Beschäftigten verifiziert werden können.

15. Vorsicht Phishing

Es können vermehrt Phishing E-Mails auftreten, die aktuelle Krisen-Situationen ausnutzen und versuchen werden, Ihre sensiblen Daten mit Hinweis auf Remote-Zugänge, das Zurücksetzen von Passwörtern etc. abzugreifen.

Das BSI stellt mit dem IT-Grundschutz-Kompendium 2020 weiterführende Informationen zu dem Thema sichere Telekommunikationsverbindungen und Telearbeit zur Verfügung.
[1;2;3;4, 5]

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_2_4_Telearbeit_Edition_2021.pdf

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_7_Informationssicherheit_auf_Auslandsreisen_Edition_2021.pdf

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/10_INF_Infrastruktur/INF_8_Haeuslicher_Arbeitsplatz_Edition_2021.pdf

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/10_INF_Infrastruktur/INF_9_IT_Mobiler_Arbeitsplatz_Edition_2021.pdf

Deutschland.Digital.Sicher.BSI