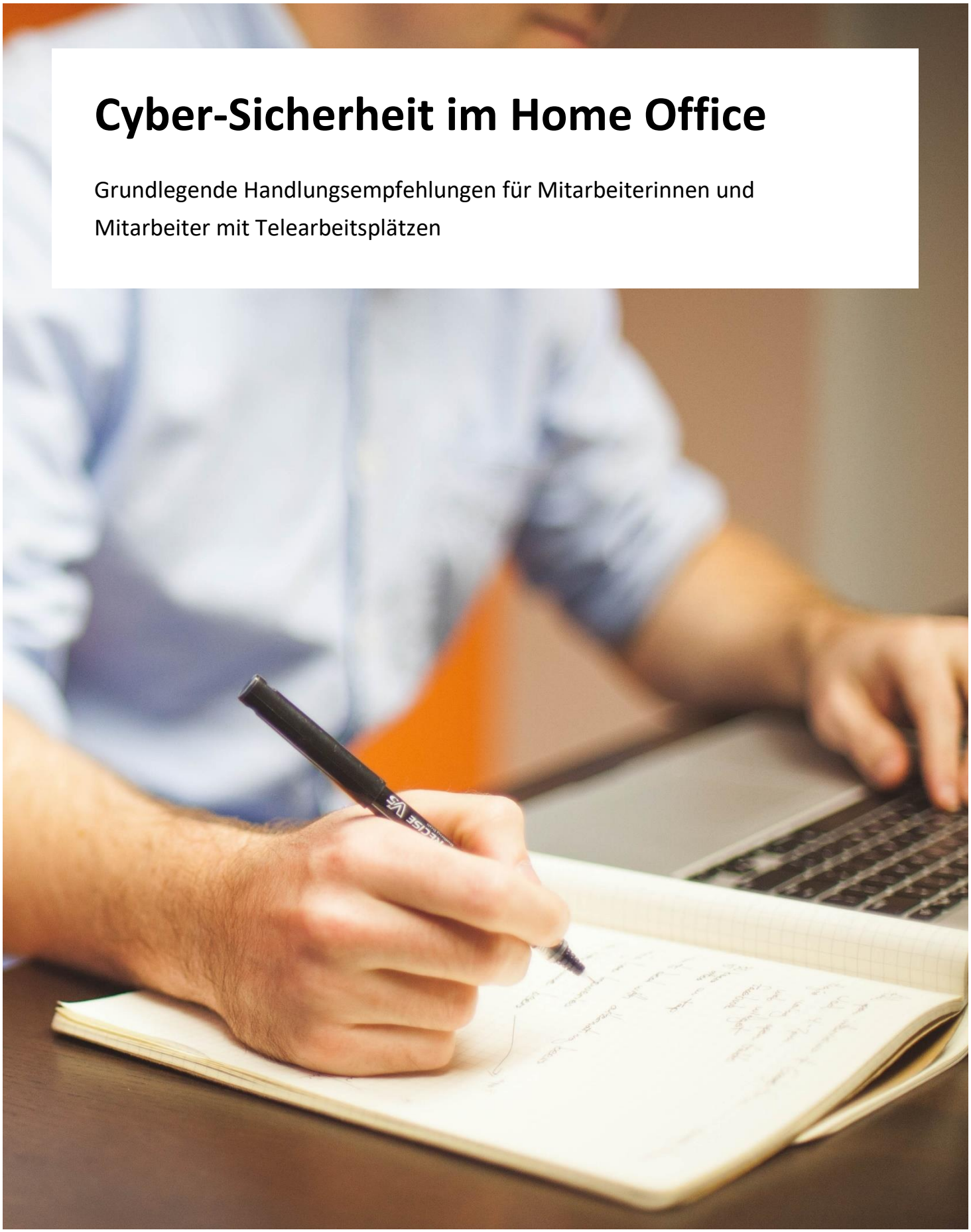
Bundesministerium
Inneres

Cyber-Sicherheit im Home Office

Grundlegende Handlungsempfehlungen für Mitarbeiterinnen und Mitarbeiter mit Telearbeitsplätzen



Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
bmi.gv.at
Autoren: Abteilung IV/10 – Netz- und Informationssystemsicherheit
Direktion Staatsschutz und Nachrichtendienst
Druck: Digitalprintcenter des BMI

Neuauflage
Wien, Februar 2022

Copyright und Haftung:
Auszugsweiser Abdruck ist nur mit Quellenangabe gestattet, alle sonstigen Rechte sind ohne schriftliche Zustimmung des Medieninhabers unzulässig.
Es wird darauf verwiesen, dass alle Angaben in dieser Publikation trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Bundesministeriums für Inneres und des Autors ausgeschlossen ist. Rechtausführungen stellen die unverbindliche Meinung des Autors dar und können der Rechtsprechung der unabhängigen Gerichte keinesfalls vorgreifen.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an praevention@nis.gv.at | csc@dsn.gv.at

Vorwort

Das sogenannte Home Office, also diejenige Form der Telearbeit, bei der Mitarbeiterinnen und Mitarbeiter einer Organisation ihre Arbeitsleistung in der eigenen Wohnung erbringen, erfreut sich in Österreich schon seit längerer Zeit wachsender Beliebtheit. Für die Kommunikation zwischen Unternehmen und Telearbeitsplätzen werden dabei in der Regel digitale Informationskanäle genutzt. Dabei ist zu bedenken, dass hier mitunter sensible Daten, die ansonsten den geschützten Firmenbereich niemals verlassen, über das öffentliche Internet übermittelt werden.

Eine wichtige Grundlage der erfolgreichen Einführung dieser Arbeitsform ist, dass sowohl den Unternehmen wie auch den Mitarbeiterinnen und Mitarbeitern eine ausreichende Zeitspanne zur Vorbereitung und Implementierung der erforderlichen technischen Vorraussetzungen zur Verfügung steht. Durch die Entwicklungen im Zusammenhang mit der weltweiten Ausbreitung des COVID-19-Virus sehen wir uns derzeit mit der Situation konfrontiert, dass bei vielen Unternehmen in Österreich Home Office-Lösungen eingeführt werden müssen. Den Unternehmen, aber vor allem den betroffenen Mitarbeiterinnen und Mitarbeitern, bleibt wenig bis keine Zeit, sich mit den Sicherheitsanforderungen auseinanderzusetzen. Dies stellt die Verantwortlichen in den Unternehmen und auch die Mitarbeiterinnen und Mitarbeiter mitunter vor neue Herausforderungen.

Aus diesem Grund haben wir uns kurzfristig entschlossen, wesentliche Grundlagen für den sicheren Einsatz von Home Office-Lösungen mit einem Fokus auf die betroffenen Mitarbeiterinnen und Mitarbeiter in diesem Dokument zusammenzustellen. Dabei stehen alle Informationen sowohl in Form von umfassenden Erläuterungen, als auch in Form von zusammengefassten Handlungsempfehlungen zur Verfügung.

Bitte beachten Sie, dass es sich bei diesem Dokument um allgemeine Empfehlungen handelt. Vorhandene Richtlinien und Policies in Ihrem Unternehmen sind jedenfalls zu beachten.

Inhalt

1 Zusammenfassung der Handlungsempfehlungen

Bei den in diesem Abschnitt angeführten Handlungsempfehlungen handelt es sich um die Schlussfolgerungen der korrespondierenden Abschnitte in diesem Dokument. Details und Hintergründe der jeweiligen Handlungsempfehlungen finden Sie im entsprechenden Abschnitt.

Cyber-Sicherheit am Arbeitsgerät

Physische Sicherheit

- Stellen Sie in den Zeiten aktiven Arbeitens sicher, dass Ihr Arbeitsplatz weder von Dritten eingesehen werden kann (Blickschutz), noch, dass dienstliche Kommunikation von Dritten mitgehört werden kann (Mitbewohnerinnen oder Mitbewohner, offene Fenster, Sprachassistenten).
- Stellen Sie in inaktiven Zeiten eine gesicherte Verwahrung aller Arbeitsgeräte sicher.
- Sorgen Sie beim vorübergehenden Verlassen des Heimarbeitsplatzes für eine geeignete Sperre Ihrer Arbeitsgeräte.

Festplatten-Verschlüsselung

- Stellen Sie sicher, dass alle Datenträger, mit denen Sie einen gesicherten Bereich verlassen, stets verschlüsselt sind.
- Bedenken Sie, dass dies nicht nur Notebooks, sondern beispielsweise auch externe Festplatten und USB-Speichersticks betrifft.

Sicherheits-Updates

- Spielen Sie alle für Ihre Arbeitsgeräte verfügbaren Sicherheits-Updates gewissenhaft und zeitnah ein.
- Werden Sie nach einem Sicherheits-Update von Ihrem System zu einem Neustart aufgefordert, sollten Sie diesen möglichst zeitnah durchführen.

- Deaktivieren Sie auf keinen Fall Funktionalitäten zum automatisierten Einspielen von Sicherheits-Updates.
- Setzen Sie keine Software ein, die vom Hersteller nicht mehr mit Updates oder Patches versorgt wird.

Absicherung des Arbeitsgerätes

- Sichern Sie Ihr Arbeitsgerät mit Antivirensoftware und Firewall ab und deaktivieren Sie diese Programme keinesfalls.
- Halten Sie Ihre Antivirensoftware stets auf dem aktuellen Stand.

Verbindung mit dem Firmenstandort

Einrichtung einer sicheren Verbindung

- Greifen Sie ausschließlich über ein kryptographisch abgesichertes Virtual Private Network (VPN) auf das Unternehmensnetzwerk zu.
- Befolgen Sie alle Sicherheitsrichtlinien und Policies Ihres Unternehmens und führen Sie keinesfalls eigenmächtig Konfigurationsänderungen am VPN durch.
- Verwenden Sie ausschließlich die von Ihrem Unternehmen zur Verfügung gestellte Software.

Mehrfaktor-Authentifizierung

- Wenn Ihnen bei der Nutzung eines Dienstes die Möglichkeit einer Mehrfaktor-Authentifizierung zur Verfügung gestellt wird, sollten Sie diese auf jeden Fall verwenden.

E-Mail Verschlüsselung

- Unverschlüsselte E-Mails sind kein adäquates Medium, um vertrauliche Informationen über das öffentliche Internet auszutauschen.
- Befolgen Sie im Zusammenhang mit dem Versenden von E-Mails alle Richtlinien und Policies Ihres Unternehmens.

Datenspeicherung

- Speichern Sie alle Daten nach Möglichkeit ausschließlich auf Servern im Unternehmensnetzwerk und greifen Sie über den Kommunikationskanal auf diese zu.
- Speichern Sie Daten nur im Ausnahmefall auf Ihrem lokalen Arbeitsgerät. Erstellen Sie in diesem Fall regelmäßig Sicherheitskopien der Daten und verwahren Sie diese an einem sicheren Ort.

Sicheres Verhalten

Exklusive Nutzung des Arbeitsgerätes

- Trennen Sie strikt zwischen dienstlichen und privaten Aufgaben und verwenden Sie nach Möglichkeit die Arbeitsgeräte des Home Office nicht für private Aktivitäten.
- Weichen Sie für die private Internetnutzung nach Möglichkeit auf alternative Geräte aus.
- Stellen Sie sicher, dass die Arbeitsgeräte auch in Ihrer Abwesenheit nicht durch Dritte (z. B. Familienmitglieder) benutzt werden können.

Kennwortsicherheit

- Verwenden Sie stets starke Kennwörter, die Sie sich jedoch noch merken können.
- Ist es erforderlich, Zugangsdaten niederzuschreiben, verwahren Sie diese Unterlagen stets an einem sicheren Ort (z. B. Safe).
- Geben Sie Ihre persönlichen Zugangsdaten ausnahmslos an niemanden weiter.

Social Engineering

- Befolgen Sie niemals Anweisungen eines unbekannten Anrufers bzw. geben Sie niemals vertrauliche Daten (z. B. Zugangsdaten) an unbekannte Anrufer weiter.
- Wenn Sie im Zusammenhang mit der Home Office-Nutzung an unerwarteter Stelle bzw. zu einem unerwarteten Zeitpunkt zur Eingabe von Zugangsdaten aufgefordert werden, sollten Sie dies vor einer etwaigen Eingabe mit Ihrem Unternehmen verifizieren.

- Führen Sie keine eigenmächtigen Softwareinstallationen (z. B. Fernwartungssoftware) oder Konfigurationsänderungen an den Kommunikationskanälen zum Unternehmen durch, außer es handelt sich um einen zuvor verifizierten Auftrag eines berechtigten Unternehmensvertreters.

Phishing & Co

- Behandeln Sie unerwartete E-Mails oder E-Mails von unbekannten Absendern mit einem gesunden Maß an Skepsis.
- Machen Sie sich bewusst, dass Absenderadressen von E-Mails vergleichsweise leicht gefälscht werden können und keinesfalls wirklich vom angegebenen Absender stammen müssen.
- Öffnen Sie keine fragwürdigen E-Mail-Attachments und klicken Sie niemals auf Hyperlinks in E-Mails.

Nutzung von USB-Speichersticks

- Schließen Sie keine unbekannten USB-Geräte (insbesondere USB-Speichersticks) an Ihr Arbeitsgerät an.

2 Cyber-Sicherheit am Arbeitsgerät

Cybersicheres Arbeiten im Home Office ist, unabhängig davon, ob das Arbeitsgerät über digitale Kommunikationskanäle mit dem Firmenstandort verbunden ist oder nur lokal genutzt wird, grundsätzlich nur möglich, wenn das betreffende Arbeitsgerät selbst sicher ist.

2.1 Physische Sicherheit

Ein grundlegendes Element des sicheren Betriebs eines Home Office ist die physische Sicherheit des Arbeitsgerätes. Es ist zu bedenken, dass bei jeder Form der Telearbeit mitunter sensible Daten, die ansonsten den geschützten Firmenbereich niemals verlassen, über das öffentliche Internet übermittelt und/oder auf Geräten außerhalb des physischen Einflussbereichs des Unternehmens bearbeitet und gespeichert werden.

Es sollte daher angestrebt werden, auch am Telearbeitsplatz ein Sicherheitsniveau herzustellen, das möglichst mit dem Firmenstandort vergleichbar ist. Insbesondere ist darauf zu achten, dass die Arbeitsgeräte im Home Office vor unberechtigtem Zugriff geschützt werden.

Stellen Sie in den Zeiten aktiven Arbeitens sicher, dass Ihr Arbeitsplatz weder von Dritten eingesehen werden kann, noch, dass dienstliche Kommunikation von Dritten mitgehört werden kann. Dies ist vor allem, aber nicht ausschließlich, im Zusammenhang mit Mitbewohnerinnen oder Mitbewohnern, offenen Fenstern und dem Vorhandensein von Sprachassistenten im Hörbereich des Arbeitsplatzes relevant. In inaktiven Zeiten ist eine sorgfältige und sichere Aufbewahrung aller Arbeitsgeräte (z. B. Notebook, externe Festplatten, USB-Speichersticks) unbedingt sicherzustellen.

Wenn der Heimarbeitsplatz vorübergehend verlassen wird, sollte auf eine geeignete Sperre der Arbeitsgeräte und im Bestfall des Arbeitsraumes geachtet werden. Dies verhindert einen missbräuchlichen Zugriff anwesender Dritter auf die Daten.

Wir empfehlen:

- Stellen Sie in den Zeiten aktiven Arbeitens sicher, dass Ihr Arbeitsplatz weder von Dritten eingesehen werden kann (Blickschutz), noch, dass dienstliche Kommunikation von Dritten mitgehört werden kann (Mitbewohnerinnen oder Mitbewohner, offene Fenster, Sprachassistenten).
- Stellen Sie in inaktiven Zeiten eine gesicherte Verwahrung aller Arbeitsgeräte sicher.
- Sorgen Sie beim vorübergehenden Verlassen des Heimarbeits-platzes für eine geeignete Sperre Ihrer Arbeitsgeräte.

2.2 Verschlüsselung von Datenträgern

Grundsätzlich sollten alle Datenträger, mit denen man einen gesicherten Bereich verlässt, verschlüsselt sein. Dies betrifft sowohl Notebooks, als auch externe Festplatten und USB-Speichersticks. Dadurch sind im Fall von Verlust oder Diebstahl, sofern das Notebook zu diesem Zeitpunkt ausgeschaltet war, zumindest die darauf gespeicherten Daten vor Ausspähung und Missbrauch sicher.

Bei Notebooks findet dabei zumeist die Windows-eigene Anwendung Bitlocker Verwendung. Steht diese Anwendung nicht zur Verfügung, können frei erhältliche und quelloffene Alternativen wie beispielsweise VeraCrypt (https://www.veracrypt.fr)[1] verwendet werden.

[1] In diesem Dokument namentlich genannte Produkte und Dienste sind lediglich als Beispiele zu verstehen und stellen keine Empfehlung durch das Bundesministerium für Inneres (BMI) dar. Das BMI hat keinerlei direkte oder indirekte Verbindung zu den jeweiligen Herstellern bzw. Betreibern und kann daher keine Garantie für die Funktion und die Sicherheit des jeweiligen Produkts bzw. Dienstes übernehmen.

Wir empfehlen:

- Stellen Sie sicher, dass alle Datenträger, mit denen Sie einen gesicherten Bereich verlassen, stets verschlüsselt sind.
- Bedenken Sie, dass dies nicht nur Notebooks, sondern beispielsweise auch externe Festplatten und USB-Speichersticks betrifft.

2.3 Sicherheits-Updates

Sicherheitslücken in Programmen werden von Angreifern genutzt, um Schadcodes in ein Gerät einzuschleusen und auszuführen. Der einzige Schutz vor der Ausnutzung von Sicherheitslücken durch Angreifer ist, diese so schnell wie möglich aus dem System zu entfernen. Softwarehersteller versuchen, neu entdeckte Sicherheitslücken durch die Verteilung von Sicherheits-Updates oder Service Packs zu bereinigen.

Aus Benutzersicht bedeutet das, dass alle offiziell verfügbaren Updates (vor allem für Betriebssystem und Internetbrowser) gewissenhaft und zeitnah einzuspielen sind. Diese Updates sollten ausschließlich aus der Software selbst heraus ausgeführt werden. Keinesfalls sollten Links auf unbekannten Webseiten oder in E-Mails zum Ausführen eines Updates verwendet werden. In einer Vielzahl von Fällen kann das Sicherheits-Update auch automatisiert durch die jeweilige Software selbst erfolgen. Solche Funktionalitäten dürfen auf keinen Fall deaktiviert werden.

In manchen Fällen ist nach der Installation eines Sicherheits-Updates ein Neustart des Systems erforderlich. Dieser sollte so zeitnah wie möglich durchgeführt und nicht verschoben werden, da manche Sicherheits-Updates erst durch einen Neustart aktiviert werden.

Zuletzt ist zu beachten, dass Softwarehersteller nur für einen begrenzten Zeitraum Ressourcen zur Verbesserung von Sicherheitslücken zur Verfügung stellen. Sicherheitslücken, die nach diesem Zeitraum entdeckt werden, bleiben bestehen und stellen von da an ein permanentes Risiko dar. In vernetzten Systemen sollte daher keine Software eingesetzt werden, die vom Hersteller nicht mehr mit Updates oder Patches versorgt wird.

Wir empfehlen:

- Spielen Sie alle für Ihre Arbeitsgeräte verfügbaren Sicherheits-Updates gewissenhaft und zeitnah ein.
- Werden Sie nach einem Sicherheits-Update von Ihrem System zu einem Neustart aufgefordert, sollten Sie diesen möglichst zeitnah durchführen.
- Deaktivieren Sie auf keinen Fall Funktionalitäten zum automatisierten Einspielen von Sicherheits-Updates.
- Setzen Sie keine Software ein, die vom Hersteller nicht mehr mit Updates oder Patches versorgt wird.

2.4 Absicherung des Arbeitsgerätes

Zwei wesentliche Elemente zum Schutz eines Arbeitsgerätes sind Antivirensoftware und (Desktop-)Firewall. Antivirensoftware vergleicht dabei hauptsächlich, aber nicht ausschließlich, Dateien auf Datenträgern mit Mustern bereits bekannter Schadsoftware und alarmiert den Benutzer bei einer etwaigen Übereinstimmung. Dies setzt voraus, dass sich die Antivirensoftware stets am neuesten Stand befindet. Eine entsprechende automatisierte Update-Funktion darf dabei in keinem Fall deaktiviert werden.

Im Unterschied zu Antivirensoftware überwacht eine Firewall im Wesentlichen die auf dem Arbeitsgerät vorhandenen Programme und erkennt, ob diese versuchen, unberechtigt auf das Internet zuzugreifen oder ob sie aus diesem kontaktiert werden. Eine einfache Firewall gehört zur Standardinstallation von Windows und sollte keinesfalls deaktiviert werden.

Wir empfehlen:

- Sichern Sie Ihr Arbeitsgerät mit Antivirensoftware und Firewall ab und deaktivieren Sie diese Programme keinesfalls.
- Halten Sie Ihre Antivirensoftware stets auf dem aktuellen Stand.

3 Verbindung mit dem Firmenstandort

In den seltensten Fällen erfolgt die Arbeit im Home Office nur lokal am Arbeitsgerät. In der überwiegenden Mehrzahl der Anwendungsfälle ist der Telearbeitsplatz über digitale Kommunikationskanäle an das jeweilige Firmennetzwerk angebunden. Die Cyber-Sicherheit dieser Verbindung muss dabei stets sichergestellt sein.

3.1 Einrichtung einer sicheren Verbindung

Greift man aus dem Home Office über das öffentliche Internet auf das Unternehmensnetzwerk zu, sollte dies keinesfalls über eine unverschlüsselte Verbindung, sondern über ein sogenanntes Virtual Private Network (VPN) erfolgen. Bei einem VPN wird zwischen dem eigenen Endgerät und dem Unternehmensnetzwerk ein durch starke Kryptographie abgesicherter Kanal aufgebaut. Die gesamte Kommunikation mit dem Unternehmen erfolgt ausschließlich über diesen Kanal und ist somit für einen Angreifer im öffentlichen Internet nicht mehr verfolgbar.

Die Einrichtung eines Virtual Private Networks kann nur in Zusammenarbeit mit dem IKT-Bereich des Unternehmens anhand der im Unternehmen gültigen Richtlinien und Policies erfolgen. Dabei ist es entscheidend, klare Regelungen zur Nutzung festzulegen und diese allen Beteiligten zur Kenntnis zu bringen. Insbesondere sollte festgehalten werden, wer auf welchem Weg Aufträge zu Konfigurationsänderungen kommunizieren darf. Weiters sollte es definierte und bekanntgemachte Kontaktstellen für Rückfragen geben.

Im technischen Bereich sollte sichergestellt werden, dass die gesamte benötigte Software (z. B. VPN-Clientsoftware) sowie die erforderlichen Zertifikate ausschließlich vom Arbeitgeber zur Verfügung gestellt und nicht von den Mitarbeiterinnen und Mitarbeitern aus dem Internet bezogen werden.

Wir empfehlen:

- Greifen Sie ausschließlich über ein kryptographisch abgesichertes Virtual Private Network (VPN) auf das Unternehmensnetzwerk zu.
- Befolgen Sie alle Sicherheitsrichtlinien und Policies Ihres Unternehmens und führen Sie keinesfalls eigenmächtig Konfigurationsänderungen am VPN durch.
- Verwenden Sie ausschließlich die von Ihrem Unternehmen zur Verfügung gestellte Software.

3.2 Mehrfaktor-Authentifizierung

Eine Authentifizierung, also der Nachweis der eigenen Identität gegenüber einem beliebigen System, kann grundsätzlich auf drei verschiedenen, sogenannten Faktoren beruhen:

- **Etwas, das ich weiß**: Für eine Authentifizierung ist lediglich die Kenntnis der jeweiligen Zugangsdaten erforderlich (z. B. Kennwort, PIN-Code, Mobiltelefon-Wischmuster).
- **Etwas, das ich habe**: Für eine Authentifizierung ist das Vorhandensein eines physischen Gegenstandes erforderlich (z. B. Token-Generator, Keycard). Auch das beim jeweiligen Geldinstitut registrierte Mobiltelefon beim mTAN-Verfahren (Online-Banking) zählt zu diesem Faktor.
- **Etwas, das ich bin**: Zur Authentifizierung werden körperliche Merkmale des Benutzers herangezogen (z. B. Fingerabdruck, Venenmuster, IRIS- oder Retinaabbild).

Wenn für einen Authentifizierungsvorgang Daten aus zumindest zwei unterschiedlichen Faktoren erforderlich sind, spricht man von Mehrfaktor-Authentifizierung (z. B. Fingerabdruck und Kennwort, Kennwort und mTAN). Mehrfaktor-Authentifizierung erhöht die Sicherheit eines Anmeldevorgangs erheblich und sollte daher überall dort genutzt werden, wo sie zur Verfügung steht.

Wir empfehlen:

- Wenn Ihnen bei der Nutzung eines Dienstes die Möglichkeit einer Mehrfaktor-Authentifizierung zur Verfügung gestellt wird, sollten Sie diese auf jeden Fall verwenden.

3.3 E-Mail Verschlüsselung

Unverschlüsselte E-Mails sind kein adäquates Medium, um vertrauliche Informationen über das öffentliche Internet auszutauschen. Eine unverschlüsselte E-Mail ist mit einer Postkarte vergleichbar. Jeder Server in der Kette zwischen Sender und Empfänger kann die über ihn transportierten Nachrichten einsehen und manipulieren.

Ein Problem im Zusammenhang mit E-Mail-Verschlüsselung ist die inkonsistente Verwendung der entsprechenden Begrifflichkeiten:

- **Verschlüsselter E-Mail-Abruf**: Bei der Einrichtung der eigenen E-Mail-Anwendung (z. B. Microsoft Outlook) kann eingestellt werden, dass die Abfrage von E-Mails verschlüsselt erfolgen muss. Das bedeutet jedoch nur, dass der Übertragungsweg zwischen dem Mail-Server und der E-Mail-Anwendung verschlüsselt wird, nicht jedoch der gesamte verbleibende Übertragungsweg.
- **end2end-Verschlüsselung**: Umfassende Sicherheit für den gesamten Übertragungsweg bietet lediglich die end2end-Verschlüsselung. Hier vereinbaren in der Regel die beiden E-Mail-Anwendungen miteinander eine Verschlüsselung, die den gesamten Übertragungsweg beinhaltet. Die Technologie der Wahl ist hier ein sogenanntes asymmetrisches (Public-Private-Key)-Verschlüsselungsverfahren. Die gängigen Standards zu dieser Technologie heißen S-MIME bzw. PGP.

Die Einrichtung einer end2end-Verschlüsselung kann nur in Zusammenarbeit mit dem IKT-Bereich des Unternehmens anhand der im Unternehmen gültigen Richtlinien und Policies erfolgen.

Wir empfehlen:

- Unverschlüsselte E-Mails sind kein adäquates Medium, um vertrauliche Informationen über das öffentliche Internet auszutauschen.
- Befolgen Sie im Zusammenhang mit dem Versenden von E-Mails alle Richtlinien und Policies Ihres Unternehmens.

3.4 Datenspeicherung

Bei der Datenspeicherung müssen die Anforderungen sowohl der Vertraulichkeit, als auch der Verfügbarkeit sichergestellt sein. Das bedeutet, dass einerseits die Sicherheit vor Ausspähung, andererseits aber auch die Datensicherheit in Bezug auf Verlust oder Kompromittierung berücksichtigt werden muss.

Die zu bevorzugende Methode, um beiden Anforderungen gerecht zu werden, stellt die ausschließliche Speicherung von Daten im Firmennetzwerk dar. Dazu wird für die Bearbeitung der Daten aber ein aufrechter Kommunikationskanal mit dem Unternehmen benötigt. Steht dieser vorübergehend nicht zur Verfügung, muss im Ausnahmefall auf die lokale Speicherung von Daten ausgewichen werden. In diesem Fall sollten regelmäßig Sicherheitskopien der Daten hergestellt und an einem sicheren Ort verwahrt werden.

Wir empfehlen:

- Speichern Sie alle Daten nach Möglichkeit ausschließlich auf Servern im Unternehmensnetzwerk und greifen Sie über den Kommunikationskanal auf diese zu.
- Speichern Sie Daten nur im Ausnahmefall auf Ihrem lokalen Arbeitsgerät. Erstellen Sie in diesem Fall regelmäßig Sicherheitskopien der Daten und verwahren Sie diese an einem sicheren Ort.

4 Sicheres Verhalten

Neben der Sicherheit des Arbeitsgerätes und des Kommunikationskanals ist es von entscheidender Bedeutung, dass die Mitarbeiterinnen und Mitarbeiter im Home Office eine Reihe von allgemeinen Verhaltensweisen einhalten.

4.1 Exklusive Nutzung des Arbeitsgerätes

Während es bei dienstlichen Arbeitsgeräten auch bisher schon zumeist unzulässig war, diese für private Zwecke zu nutzen, so stellt die nunmehr verbreitete Situation, wonach in verstärktem Maße private Endgeräte für Home Office-Aufgaben herangezogen werden, eine neue Herausforderung dar.

Bei einem dienstlichen Arbeitsgerät (z. B. Firmennotebook) war es in der Regel schon bisher gelebte Praxis, dass eine Benutzung durch Dritte sowie eine Nutzung für nichtdienstliche Zwecke unzulässig war. Kommt nunmehr ein privates Endgerät im Einvernehmen mit dem Unternehmen für Home Office-Aufgaben zum Einsatz, so sollten diese Regelungen nach Möglichkeit auch auf diese angewandt werden. Weichen Sie für die private Internetnutzung nach Möglichkeit auf alternative Geräte aus.

Insbesondere die Nutzung durch Kinder und Jugendliche ohne ausgebildetes Sicherheitsbewusstsein in Abwesenheit des Unternehmensmitarbeiters stellt in diesem Zusammenhang ein unkalkulierbares Risiko für die Integrität des Gerätes dar.

Wir empfehlen:

- Trennen Sie strikt zwischen dienstlichen und privaten Aufgaben und verwenden Sie nach Möglichkeit die Arbeitsgeräte des Home Office nicht für private Aktivitäten.
- Weichen Sie für die private Internetnutzung nach Möglichkeit auf alternative Geräte aus.
- Stellen Sie sicher, dass die Arbeitsgeräte auch in Ihrer Abwesenheit nicht durch Dritte (z. B. Familienmitglieder) benutzt werden können.

4.2 Kennwortsicherheit

Kennwortsicherheit ist ein zentrales Thema im Zusammenhang mit Cyber-Sicherheit, auch und vor allem im Zusammenhang mit der Nutzung im Rahmen von Telearbeitsplätzen. Bei der Kennwortwahl sollten folgende Gefahrenquellen berücksichtigt werden:

- **„zu einfach“**: Ist ein Kennwort zu schwach, kann es leicht erraten oder durch Ausprobieren kompromittiert werden.
- **„zu komplex“**: Zugangsdaten, die man sich nicht merken kann, werden oft aufgeschrieben und an unsicheren Orten aufbewahrt.
- **„one4all“**: Werden ein- und dieselben Zugangsdaten für mehrere Accounts genutzt, bedeutet die Kompromittierung eines Accounts auch, dass alle anderen Accounts kompromittiert werden können.
- **„4ever“**: Werden Kennwörter nicht regelmäßig geändert, kann ein Angreifer, sobald er Kenntnis von einem Kennwort hat, dieses auch in Zukunft unbemerkt missbrauchen.

Grundsätzlich gilt, dass die Sicherheit eines Kennworts mit steigender Länge und Komplexität zunimmt (sofern der Benutzer noch in der Lage ist, sich das entsprechende Kennwort zu merken). Kennwörter in sensiblen Bereichen sollten derzeit eine Mindestlänge von 12 Stellen bei hoher Komplexität (d.h. Klein- und Großbuchstaben, Ziffern, Sonderzeichen) aufweisen.

Kennwörter müssen insbesondere aus den folgenden Gründen als schwach bzw. unsicher eingestuft werden:

- **Mangelnde Kennwortlänge oder –komplexität**: Kennwörter, die eine zu geringe Stellenanzahl oder Komplexität aufweisen, können von Angreifern durch das automatisierte Durchprobieren aller möglichen Zeichenkombinationen (Brute Force-Angriff) vergleichsweise schnell gehackt werden.
- **Wörter aus Wörterbüchern**: Oft geht einem Brute Force-Angriff ein sogenannter Wortlisten-Angriff (Dictionary Attack) voraus. Dabei werden vor dem aufwändigen Durchprobieren aller möglichen Zeichenkombinationen alle Wörter aus gängigen Wörterbüchern durchprobiert. Bei Wörterbüchern in diesem Sinne muss es sich allerdings nicht ausschließlich um natürlich sprachige Wörterbücher handeln. Vielmehr sind hier beliebige Listen potentieller Kennwörter mit zu betrachten. Im Internet kursieren viele derartige Listen, die Millionen von potentiellen Kennwörtern

enthalten. Dazu gehören auch typische Tastaturmuster, Teile aus bekannten Liedern und Texten, sowie davon abgeleitete Kennwörter.

- **Sprechende Schemata**: Unbedingt zu vermeiden sind weiters sprechende Schemata als Kennwörter, die einem einheitlichen, sichtbaren Schema folgen.
- **Persönliche Daten**: Die Verwendung von persönlichen Daten als Bestandteil von Kennwörtern (z. B. Namen von Partnern, Kindern oder Haustieren, Kosenamen, Geburtsdaten oder Autonummern) sollte unbedingt vermieden werden.

Abschließend ist festzuhalten, dass persönliche Zugangsdaten in keinem Fall an eine andere Person weitergegeben werden dürfen.

Wir empfehlen:

- Verwenden Sie stets starke Kennwörter, die Sie sich jedoch noch merken können.
- Ist es erforderlich, Zugangsdaten niederzuschreiben, verwahren Sie diese Unterlagen stets an einem sicheren Ort (z. B. Safe).
- Geben Sie Ihre persönlichen Zugangsdaten ausnahmslos an niemanden weiter.

4.3 Social Engineering

Technologie alleine kann Sie nicht vollständig vor Angriffen schützen. Gerade in der aktuellen Situation ist zu erwarten, dass Angreifer versuchen werden, die fehlende Vertrautheit der Mitarbeiterinnen und Mitarbeiter mit dem Konzept des Home Office für Angriffe auszunutzen.

Vor allem das Telefon ist ein sehr verbreitetes Angriffsmittel bei solchen sogenannten „Social Engineering“-Angriffen, da sich Angerufene mangels einer face2face-Situation in der Regel leichter von vorgespiegelten Sachverhalten überzeugen lassen. Als Grundsatz gilt, dass man in solchen Situationen niemals die Anweisungen eines unbekannten Anrufers befolgen bzw. vertrauliche Daten (z. B. Zugangsdaten) an unbekannte Anrufer weitergeben sollte. Vor allem in Situationen, in denen der Anrufer vorgibt, im Auftrag Ihres Unternehmens zu handeln, empfiehlt es sich, diese Behauptung vor einer Befolgung der Anweisungen gesichert zu verifizieren.

Darüber hinaus ist zu befürchten, dass sich Angreifer die gerade in der Anfangszeit mangelnde Vertrautheit der neuen Home Office-Benutzer mit den technischen Grundlagen dieser Arbeitsform zunutze machen. So sind verstärkt gefälschte E-Mails an Mitarbeiterinnen und Mitarbeiter im Home Office zu erwarten, die vermeintlich vom eigenen Unternehmen stammen und die Nutzer zu bestimmten Aktivitäten auffordern.

Vor allem folgende Aktivitäten stellen ein erhebliches Risiko dar und sollten ausschließlich aufgrund eines zuvor verifizierten Auftrags eines dazu berechtigten Unternehmensvertreters durchgeführt werden:

- Installation von neuer Software im Zusammenhang mit der Home Office-Nutzung (z. B. Fernwartungssoftware)
- Konfigurationsänderungen an den Kommunikationskanälen zum Unternehmen
- Eingabe Ihrer Zugangsdaten an einer unerwarteten Stelle bzw. zu einem unerwarteten Zeitpunkt (z. B. auf einer externen Website)

Mitarbeiterinnen und Mitarbeiter sollten sich in Zweifelsfällen zur Verifizierung unbedingt an zuvor definierte und bekanntgemachte Kontaktstellen wenden.

Wir empfehlen:

- Befolgen Sie niemals Anweisungen eines unbekannten Anrufers bzw. geben Sie niemals vertrauliche Daten (z. B. Zugangsdaten) an unbekannte Anrufer weiter.
- Wenn Sie im Zusammenhang mit der Home Office-Nutzung an unerwarteter Stelle bzw. zu einem unerwarteten Zeitpunkt zur Eingabe von Zugangsdaten aufgefordert werden, sollten Sie dies vor einer etwaigen Eingabe mit Ihrem Unternehmen verifizieren.
- Führen Sie keine eigenmächtigen Softwareinstallationen (z. B. Fernwartungssoftware) oder Konfigurationsänderungen an den Kommunikationskanälen zum Unternehmen durch, außer es handelt sich um einen zuvor verifizierten Auftrag eines berechtigten Unternehmensvertreters.

4.4 Phishing & Co

Im engeren Sinn bezieht sich der Begriff Phishing ausschließlich auf den Versuch, an persönliche Daten (insbesondere Zugangsdaten) eines Nutzers zu gelangen, um diese dann missbräuchlich zu verwenden. Im täglichen Sprachgebrauch wird die Bedeutung allerdings für jegliche Aktivitäten benutzt, bei denen manipulierte E-Mails zum Einsatz kommen, gleichgültig, ob es dabei um das Unterschieben von Schadcode oder das Ausspähen von Zugangsdaten geht.

Beim Unterschieben von Schadcode wird der nichtsahnende Benutzer durch unterschiedliche Methoden dazu gebracht, die eingeschleuste Schadsoftware unbeabsichtigt selbst auszuführen. Die zwei häufigsten Methoden sind:

- **Manipuliertes E-Mail Attachment**: In diesem Fall sendet der Angreifer eine E-Mail an das potentielle Opfer. Diese E-Mail enthält neben dem E-Mail-Text ein manipuliertes Attachment. Der E-Mail-Text soll durch seinen Inhalt den Benutzer dazu bewegen, möglichst unbedacht auf das Attachment zu klicken und den darin enthaltenen Schadcode auszuführen.
- **Manipulierter Hyperlink**: Eine vergleichbare Methode arbeitet mit E-Mails, die Hyperlinks enthalten. Das im E-Mail-Text angezeigte Ziel eines Hyperlinks muss technisch nicht mit dem tatsächlichen Ziel übereinstimmen. Der E-Mail-Text soll durch seinen Inhalt den Benutzer dazu bewegen, auf den enthaltenen Hyperlink zu klicken. Oft zeigen solche Hyperlinks dann auf manipulierte Webserver, bei denen bereits ein bloßer Besuch der Website ausreicht, um eine Infektion auszulösen. Alternativ könnten durch einen solchen Hyperlink manipulierte Inhalte heruntergeladen werden, die ihrerseits eine Infektion auslösen.

Dabei muss sich jeder Nutzer bewusstmachen, dass die Absenderadressen von E-Mails vergleichsweise leicht gefälscht werden können und keinesfalls wirklich vom angegebenen Absender stammen müssen. Hinsichtlich möglicher Gegenmaßnahmen ist an erster Stelle der eigene Hausverstand zu nennen. Oft ist den manipulierten E-Mails bereits schon bei oberflächlicher Betrachtung anzusehen, dass es sich um keine normale Nachricht handeln kann. Entscheidend ist auch die Frage, ob es plausibel erscheint, dass man zum konkreten Zeitpunkt eine E-Mail von dem jeweiligen Absender erhält oder ob man diesen Absender überhaupt kennt. Ein gesundes Maß an Skepsis kann hier ein sehr großes Mehr an Sicherheit bewirken.

Ein Phishing-Angriff erfolgt in der Regel durch die Zusendung einer vom Angreifer vorbereiteten E-Mail oder einer Nachricht auf einer beliebigen Plattform. In dieser Nachricht wird ein bestimmtes Szenario entworfen, welches das Opfer dazu bringen soll, möglichst unmittelbar auf einen in der Nachricht eingebetteten Hyperlink zu klicken. Wie bereits ausgeführt, muss das im E-Mail-Text angezeigte Ziel eines Hyperlinks technisch nicht mit dem tatsächlichen Ziel übereinstimmen. Im Fall von Phishing wird das Opfer in Wirklichkeit auf einen Server des Angreifers umgeleitet, auf dem das eigentlich erwartete Eingabefeld für die jeweiligen Zugangsdaten (z. B. Online Banking-Eingabefeld) täuschend ähnlich nachgebaut ist. Im Glauben, seine Zugangsdaten auf einer legitimen Seite einzugeben, stellt man diese jedoch somit dem Angreifer zur Verfügung.

Wir empfehlen:

- Behandeln Sie unerwartete E-Mails oder E-Mails von unbekannten Absendern mit einem gesunden Maß an Skepsis.
- Machen Sie sich bewusst, dass Absenderadressen von E-Mails vergleichsweise leicht gefälscht werden können und keinesfalls wirklich vom angegebenen Absender stammen müssen.
- Öffnen Sie keine fragwürdigen E-Mail Attachments und klicken Sie niemals auf Hyperlinks in E-Mails.

4.5 Nutzung von USB-Speichersticks

Wird ein USB-Gerät mit einem Rechner verbunden, so teilt das Gerät dem Rechner mit, welcher Geräteklasse (z. B. Speicherstick, Tastatur, Drucker) es angehört. Dieser Information wird vom Rechner ohne weitere Überprüfung vertraut und es wird in der Folge genauso behandelt. Auf diesem Umstand baut eine Reihe von Angriffsszenarien auf, bei der mitunter das bloße Anstecken eines manipulierten USB-Gerätes bereits eine Infektion auslösen kann.

Es wird daher empfohlen, keine unbekannten USB-Geräte an den eigenen Rechner anzuschließen. Potentiell gefährliche Situationen sind dabei vielfältig:

- Gefundene USB-Geräte (z. B. in öffentlichen Verkehrsmitteln, am Firmenparkplatz, aber auch am eigenen Arbeitsplatz)

- Werbegeschenke aus unbekannten Quellen (z. B. Giveaways bei Messen/Kongressen, Straßenaktionen)
- Gefahrenquellen im Arbeitsalltag (z. B. unbekannter Besucher ersucht um Ausdruck eines auf einem USB-Speicherstick mitgebrachten Dokuments)

Dieses Gefahrenpotenzial besteht nicht nur bei USB-Speichersticks, sondern grundsätzlich bei allen Geräten, die über die USB-Schnittstelle an einen Rechner angeschlossen werden.

Wir empfehlen:

- Schließen Sie keine unbekannten USB-Geräte (insbesondere USB-Speichersticks) an Ihr Arbeitsgerät an.

Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
praevention@nis.gv.at | csc@dsn.gv.at
bmi.gv.at