Sicheres und vertrauenswürdiges Arbeiten im Homeoffice

AKTUELLE SITUATION DER CYBERSICHERHEITSLAGE

Durch die fortschreitende Digitalisierung bekommt die IT einen immer größeren Stellenwert in allen Bereichen. Dadurch steigt die Abhängigkeit von der IT und damit auch das Schadenspotenzial durch Cyberangriffe. Besonders durch die Zunahme der Arbeitsform Homeoffice sowie die Ad-hoc-Verlagerung von Beschäftigten und Geschäftsprozessen in das Homeoffice entstehen durch bisher unzureichende infrastrukturelle Sicherheitsvorkehrungen höhere Risiken. Anbieter von Video-Konferenz- und anderen Kollaborationstools haben durch den enormen Digitalisierungsschub nicht genug Zeit gehabt, ihre Systeme angemessen zu schützen. Dazu kommt, dass die Nutzung von unsicheren oder nicht ausreichend datenschutzkonformen Lösungen, wie Messenger oder sozialen Netzwerken, weitere Risiken für Unternehmen darstellen können. Welche technischen, personellen und organisatorischen Maßnahmen sind also erforderlich, um in der angespannten Lage ein sicheres Homeoffice einzurichten?

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat für das Jahr 2020 durchschnittlich etwa 320.000 neue Schadprogramm-Varianten pro Tag verzeichnet. Dabei handelte es sich unter anderen um Ransomware, Spam, Identitätsdiebstahl und Daten-Leaks. Auch führten Schwachstellen in IT-Systemen und schlechte Update-Strategien zu großen Problemen. Generell werden Cyberangriffe immer ausgereifter, besonders im Bereich der Destributed Denial of Service (DDoS) werden die Strategien der Angreifer zunehmend intelligenter.[1]

Seit Beginn der Corona-Pandemie steigt die Zahl der Homeoffice-Arbeitsplätze in Deutschland an. In einer Studie aus dem Jahre 2020 fand ESET heraus, dass letztes Jahr rund 41 Prozent aller Beschäftigten in Deutschland im Homeoffice arbeiteten. Dagegen waren im Jahr 2019 nur 12,9 Prozent im Homeoffice.[2] Rund 78 Prozent der Unternehmen wollen Homeoffice auch nach dem Ende der Pandemie weiter ermöglichen.

Daher ist es besonders relevant, neue Risiken, die durch die vermehrte Arbeit im Homeoffice entstehen, zu betrachten und ihnen entgegenzuwirken. Gefahren, wie Denial-of-Service-Angriffe, stellen im Homeoffice eine reale Bedrohung dar und können die Verbindung zur Unternehmensinfrastruktur unterbinden. Derzeit ist nur jeder zweite Homeoffice-Arbeitsplatz gegen mögliche Angriffe angemessen gesichert. Das liegt unter anderem daran, dass nur 44 Prozent der von ESET befragten Firmen in Deutschland den Zugriff der Mitarbeiter auf die Firmen-Ser-

Bild: ©pikselstock - stock.adobe.com

ver mittels einer sichereren VPN-Verbindung realisieren. Lediglich 29 Prozent verwenden Zwei-/Multi-Faktor-Authentifizierungs-Lösungen für eine zusätzliche Absicherung.[3]

DEFINITIONEN VON „HOMEOFFICE“

Derzeit wird hauptsächlich der Begriff Homeoffice verwendet. Jedoch gibt es noch andere Bezeichnungen, die das Arbeiten von zu Hause beziehungsweise außerhalb des Firmensitzes bezeichnen. Dabei ist zu beachten, welche rechtlichen Rahmenbedingungen bei der jeweiligen Form der Heimarbeit gelten. Es wird zwischen Telearbeit, Mobile Working und Homeoffice unterschieden.

Telearbeit

Die Telearbeit wird in der Arbeitsstättenverordnung geregelt: „Telearbeitsplätze sind vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten, für die der Arbeitgeber eine mit den Beschäftigten vereinbarte wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat. Ein Telearbeitsplatz ist vom Arbeitgeber erst dann eingerichtet, wenn Arbeitgeber und Beschäftigte die Bedingungen der Telearbeit arbeitsvertraglich oder im Rahmen einer Vereinbarung festgelegt haben und die benötigte Ausstattung des Telearbeitsplatzes mit Mobiliar, Arbeitsmitteln einschließlich der Kommunikationseinrichtungen durch den Arbeitgeber oder eine von ihm beauftragte Person im Privatbereich des Beschäftigten bereitgestellt und installiert ist.“ (§ 2 Nr. 7 der Arbeitsstättenverordnung). Demnach muss der Arbeitgeber den Heimarbeitsplatz komplett einrichten, sodass der Arbeitnehmer alle Möglichkeiten zur Erfüllung seiner Tätigkeit erhält. Die Telearbeit und der damit zusammenhängende Heimarbeitsplatz sind zusätzlich zu einem regulären Arbeitsplatz im Unternehmen vorhanden. Derzeit existiert noch kein Rechtsanspruch auf Telearbeit in Deutschland.

Mobile Working

Mobile Working ist nicht gesetzlich geregelt und definiert, baut aber wie die Telearbeit auf einer Verbindung zum Betrieb über IT-Endgeräte und Kommunikationsinfrastrukturen auf. Im Gegensatz zur Telearbeit ist Mobile Working nicht an einen definierten und festen Heimarbeitsplatz gebunden. Daher ist das Arbeiten theoretisch von überall möglich, sofern ein Notebook, Tablet oder Smartphone inklusive einer Kommunikationsanbindung (fest oder mobil) vorhanden ist. Außerdem ist Mobile Working nicht an feste Arbeitszeiten und Arbeitsplätze gebunden. Zunehmend wird „Mobile Working“ oft an für den Mitarbeiter besonders attraktiven Umgebungen durchgeführt – etwa im Ferienhaus auf dem Land, oder gar in schönen fernen Ländern. Beispielsweise werben Hotels in Bali mit Coworking Spaces für ausländische Arbeitnehmer. Es ist ein Trend zu erkennen, dass Mitarbeiter, die mobil arbeiten, dieses zunehmend gleichzeitig für mehrere Unternehmen tun. Auch dieser Aspekt erfordert neuartige, sichere und vertrauenswürdige IT-Arbeitsumgebungen, damit die Risiken für die unterschiedlichen Arbeitgeber reduziert werden können.

Homeoffice

Homeoffice bedeutet, dass Mitarbeiter einer Organisation oder eines Unternehmens ihre Arbeiten in privaten Räumlichkeiten und nicht im Unternehmen selbst ausüben. Dabei handelt es sich nicht um einem vom Arbeitgeber vollständig eingerichteten Arbeitsplatz. Der externe Homeoffice-Arbeitsplatz erhält über das private Internet des Arbeitnehmers Zugriff auf die Ressourcen des Arbeitgebers, beispielsweise interne IT-Infrastrukturen oder Cloud-Dienste des jeweiligen Unternehmens. Die durch die Homeoffice-Arbeitsplätze entstandenen neuen Risiken müssen durch geeignete Cybersicherheitsmaßnahmen eliminiert oder deutlich reduziert werden.[4]

(NEUE) RISIKEN BEIM HOMEOFFICE

Durch die Arbeit im Homeoffice verändern sich unterschiedlichste Aspekte des Arbeitens. Der Arbeitnehmer und der Arbeitgeber genießen Vorteile, wie die Zeitersparnis wegen der nicht notwendigen Anreise oder erhöhte Flexibilität beim Arbeiten. Allerdings wird vom Arbeitnehmer aufgrund der variierenden Arbeitszeiten sowie der Pausen und der erhöhten Ablenkung enorm viel Disziplin gefordert. Dazu kommt, dass der Arbeitnehmer nicht allein im Homeoffice ist, beispielsweise sind Störungen und Ablenkungen während der Arbeit durch Familienmitglieder oder Mitbewohner möglich. Ferner ist der Raum zum Arbeiten in der Regel stark begrenzt.

Weitere potenzielle Risikoquellen sind Software- und Hardware-Komponenten, insbesondere, wenn der Arbeitnehmer mit privaten IT-Endgeräten (PC, Notebook, PAD, Smartphone) oder Hardwarekomponenten (Router, Drucker ...) arbeitet. Software-Update-Prozesse, Back-up-Systeme etc. sind eine weitere Herausforderung.

Heimischer, privater Internet-Zugang/Nutzung

Der heimische Internet-Zugang und die dazugehörige Infrastruktur und Router stellen im Homeoffice ein Risiko für das Unternehmen dar. Abhängig vom heimischen Internet-Zugang ist die Verfügbarkeit der IT-Systeme- und Dienste des Arbeitnehmers und somit die Tätigkeit als

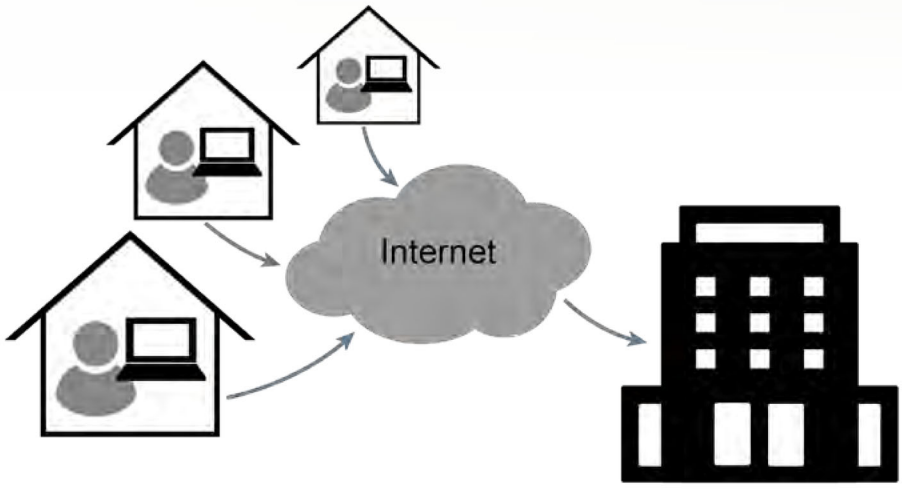

Bild 1: Homeoffice

Ressource für das Unternehmen zu betrachten. Es kann zum Beispiel eine nicht ausreichende Internet-Bandbreite und schlechte Verfügbarkeit seitens des Arbeitnehmers dazu führen, dass bestimmte Dienste nicht verwendet oder in eingeschränkter Geschwindigkeit zur Verfügung stehen.

Heimischer Router

Der heimische Router ist meist vom Arbeitnehmer konfiguriert, da dieser auf die private Nutzung ausgelegt ist. Demnach folgen die Einstellungen nicht einer möglichen Unternehmensrichtlinie und können Fehler beinhalten, die ein Risiko darstellen. Der Arbeitnehmer muss eine sichere Konfiguration des Routers vornehmen, beispielsweise durch die Verwendung eines sicheren Passworts sowie WPA2-Verschlüsselung.

Heimische Infrastruktur

Die heimische Infrastruktur stellt besonders in Häusern mit mehreren Parteien durch eine größere Angriffsfläche ein zusätzliches Risiko dar. Über den Zugang zum Hausanschlussraum oder dem Verlauf der Kabel durch andere Wohnungen ist das Mitlesen und Manipulieren der sensiblen Kommunikation möglich.[4]

Bild 2: Angriffsfläche der heimischen Infrastruktur

Smart Home

Smart Home ist in unserer heutigen Gesellschaft kaum mehr wegzudenken. Dabei ist Smart Home der Oberbegriff für die Ausgestaltung von Wohnräumen, in denen Haushalts- und Multimedia-Geräte interagieren und intelligent gesteuert werden. Smart Home hat unterschiedliche Anwendungsbereiche, wie Energiemanagement, Entertainment und Kommunikation, Gebäude- und Wohnungssicherheit, Hausautomation und Komfort, Gesundheit und ein eigenständiges Leben zu Hause auch im Alter. Jedoch bieten diese Smart-Home-Technologien neue Angriffsvektoren und Sicherheitsrisiken. Besonders im Homeoffice, bei dem private Technologien mit Teilen der Unternehmensinfrastruktur zusammenkommen, entstehen neue Einfallsvektoren für Angreifer auf die beruflich genutzte IT.[5]

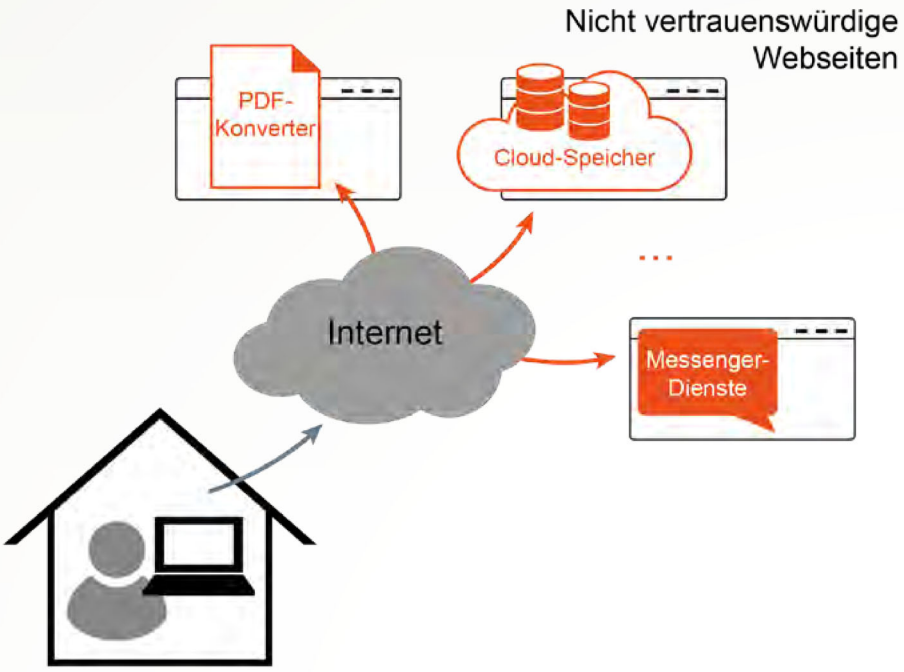

Bild 3: Schatten-IT

Einsichtnahme/Mithören

Die Möglichkeit von überall aus zu arbeiten birgt Risiken. So ermöglicht das Arbeiten an öffentlichen und teilweise einzusehenden Orten, wie Balkon oder Terrassen, Unbefugten Gespräche mitzuhören. Ebenfalls ist bei Notebook-Arbeiten Einsicht auf vertrauliche Unternehmensinformationen durch Passanten oder Nachbarn möglich.

Videokonferenz-/ Kollaborationssystem

Durch die vielen Heimarbeitsplätze ist der Bedarf an einfach zu handhabenden Videokonferenzsystemen enorm gestiegen. Mit mehr als 300 Millionen Nutzern täglich hob der Anbieter Zoom sich von der Menge der Anbieter ab. Die Schattenseiten des enormen und schnellen Wachstums gingen zulasten der Sicherheit, weshalb diverse Videokonferenzsysteme in den Medien hauptsächlich durch Schwachstellen auf sich aufmerksam machten.[6]

Schatten-IT

Schatten-IT sind IT-Systeme und -Dienste, die von Mitarbeitern neben der offiziellen IT-Infrastruktur der Unternehmen verwendet werden, um ihre Arbeit schneller und besser umsetzen zu können.

In Bild 3 wird die Nutzung von Schatten-IT dargestellt. Die Verwendung von nicht vertrauenswürdigen Webseiten oder Cloud-Diensten wie die Umwandlung in PDFs bei kostenlosen Diensten, Austausch von Dateien mittels einer Dropbox-Lösung oder Nutzung von unsicheren Chat-Systemen stellen Sicherheitsrisiken im Homeoffice dar.[4] Die Anbieter lassen sich oft durch die AGBs die Rechte auf die Daten bestätigen – für Unternehmen ein absolutes No-Go.

Angriffsvektor Mensch

Besonders Arbeitnehmer, die nicht IT-sicherheitsaffin sind, gelten als einfacher Angriffspunkt. Gerade wenn die Mitarbeiter aus dem Homeoffice arbeiten, sind sie mangels direktem

Info-Austauschmöglichkeit mit Kollegen anfälliger für Manipulationsangriffe wie Phishing oder Spam. Daher sollten Mitarbeiter geschult werden, welche Werte besonders geschützt werden müssen, wie man sich gegen Angriffe wehren kann und was zu tun ist, wenn ein Angriff erfolgreich stattgefunden hat.

TECHNISCHE IT-SICHERHEITSMASSNAHMEN

IT-Sicherheitsmaßnahmen sind alle Aktionen, die dazu dienen, vorhandene IT-Sicherheitsrisiken zu minimieren. Dies schließt sowohl organisatorische als auch personelle, technische oder infrastrukturelle IT-Sicherheitsmaßnahmen ein. Damit Unternehmen auf die neuen Risiken reagieren können, sollten technische IT-Sicherheitsmaßnahmen implementiert werden. Im Folgenden werden ein paar Beispiele aufgeführt.

Sichere Anbindung des Heimarbeitsplatzes an das Unternehmen

Das Homeoffice muss über ein VPN-System an die Institution angekoppelt werden, damit die Daten verschlüsselt und integritätsgesichert übertragen werden. Bei der Verwendung von öffentlichen WLAN-Hotspots ist eine gesicherte VPN-Verbindung unumgänglich. Eine weitere Maßnahme stellt eine sichere Konfiguration des heimischen Routers, des Internet-Zugangs und weiterer Infrastruktur (zum Beispiel Smart-Home-Anwendungen) dar.

Professionelle Router bieten darüber hinaus weitere Sicherheitsoptionen, wie eine Statefull-Packet-Inspection Firewall, DoS-Schutz und Inhaltsfilterung, an. Dabei muss der Anwender kein Experte sein, um die Einstellungen umzusetzen. Damit der Router und seine Sicherheitsoptionen einen permanenten Schutz bieten, müssen regelmäßige Firmware-Updates vorgenommen werden.[7]

Zugriffskontrolle/ Nutzerauthentifizierung

Es sollte genau definiert werden, wer worauf zugreifen darf. Dank Lösungen wie Single Sign-on (SSO) lässt sich einfach steuern, auf welche Anwendungen welcher Mitarbeit zugreifen darf. Außerdem sollte mittels eines Authentifizierungsverfahrens sichergestellt werden, dass es sich tatsächlich um den Mitarbeiter handelt, der eine Anwendung verwenden möchte. Die Nutzung einer Zwei-/Multi-Faktor-Authentifizierung (2FA/MFA) sorgt dafür, dass der Zugriff angemessen sicher für IT-Dienste des Unternehmens oder Cloud-Dienste verwendet werden kann. Auch hier gibt es schon professionelle Lösungen, die neben sicherer Identifikation und Authentifikation zusätzlich digitale Signaturen anbieten, damit die Mitarbeiter auch von zu Hause rechtssicher unterschreiben können.[9]

Verschlüsselung von Unternehmenswerten

Damit die Unternehmenswerte geschützt werden, sollten zum Beispiel alle Notebooks mithilfe einer Festplattenverschlüsselung vor unberechtigten physikalischen Zugriffen geschützt werden. Wenn ein Notebook gestohlen wird, beträgt der Schaden vielleicht 3.000 Euro (Anschaffungspreis eines neuen Notebooks und die Kosten der Einrichtung), aber die Unternehmenswerte, die in der Regel deutlich höher sind, bleiben geschützt. Ein Ordner oder eine Dateiverschlüsselung reduziert ungewollte Zugriffe auf Unternehmenswerte.

Remote-Back-ups

Im Homeoffice muss ein verschlüsselter Datenträger für Back-ups eingesetzt, aber auch ein regelmäßiger Back-up-Prozess über das VPN mit dem Unternehmen umgesetzt werden. Dies ist für die Aufrechterhaltung der Unternehmenswerte, aber auch als Schutz gegen Schäden durch Ransomware, wichtig.

Update

Um bekannt gewordene Schwachstellen in Software entgegenzuwirken, müssen feste und spontane Update-Prozesse für die genutzte Software etabliert und sichergestellt werden.

Schnittstellenkontrolle

Eine Schnittstellenkontrolle sowie eine Absicherung der Homeoffice-Netze, beispielsweise durch die Deaktivierung von USB-Ports und das korrekte Ausnutzen von Sicherheitsfunktionen des Routers, erhöht den Schutz von IT-Systemen.

Anti-Malware-Tools

Anti-Malware-Tools sollten modern sein und regelmäßig aktualisiert werden, um einen zuverlässigen Schutz gewährleisten zu können.

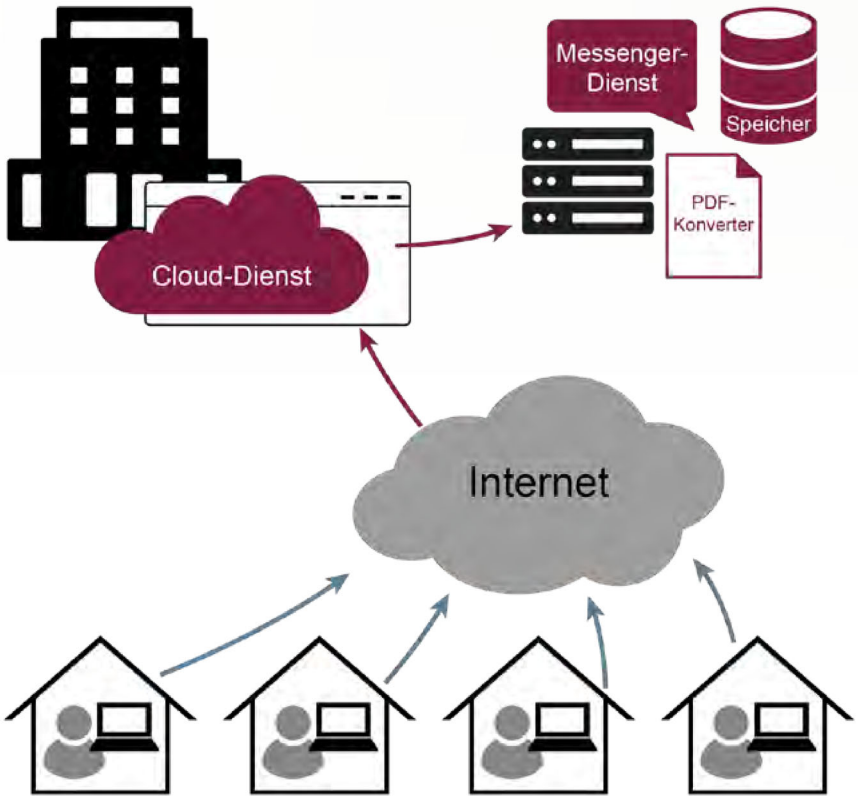

Bild 4: Mehrere Homeoffice-Systeme greifen über das Internet auf einen Cloud-Dienst der Institution zu.

Protokollierung

Die Kommunikation zum Unternehmen sollte protokolliert werden, um eine Analyse und Auswertung der Log-daten zu ermöglichen.[7]

Videokonferenz-/ Kollaborationssysteme

Besonders wichtig bei der Verwendung von Videokonferenzsystemen ist die Verschlüsselung, die mindestens End-to-End-Verschlüsselung sein muss. Ebenso sind Pre-Meeting-Einstellungen, wie Warteräume, Zutritt nur für authentifizierte Nutzer, Server des Videokonferenzsystems in der EU, zu empfehlen. Ebenso In-Meeting-Einstellungen, wie die Möglichkeit, Nutzer zu entfernen oder eintreten zu lassen, Zusatzfunktionen, wie Chat, Teilen des Bildschirmes, Zugriff auf Ressourcen, das Ändern der ID, Aktivierung von Mikrofon und Kamera sollten vom Moderator als aktiver Schutz sinnvoll genutzt beziehungsweise eingeschränkt werden.[6]

Cloud-Dienste

Die Arbeit mit Cloud-Diensten erleichtert die Zusammenarbeit im Homeoffice enorm. Neben Office- und weiteren Anwendungen können auch Messenger-Dienste oder PDF-Konverter über einen Cloud-Dienst bereitgestellt werden. Vor der Wahl eines geeigneten Cloud-Dienstes sollten die Risiken für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit überprüft werden. Darüber hinaus muss ein Cloud-Dienstanbieter vertrauenswürdig sein. Für einen Cloud-Dienst sollte ein Mindeststandard für Sicherheitsfunktionen seitens des Anbieters existieren. Zusätzlich müssen Cloud-Dienste mittels starker Verschlüsselung und zumindest durch eine 2FA/MFA geschützt werden.

Härtung von IT-Systemen

Eine technische Lösung zum Umsetzen verstärkter IT-Sicherheitsmaßnahmen im Homeoffice ist die Härtung von IT-Endgeräten. Dabei wird auf verschiedene Aspekte des IT-Endgeräts eingegangen. Eine Möglichkeit für die Härtung eines IT-Endgeräts ist die Verwendung einer Trusted Computing Base. Mittels Security Kernel, Virtualisierung und einem Trusted Software Layer können IT-Sicherheitsprinzipien durchgesetzt werden (Bild 5).

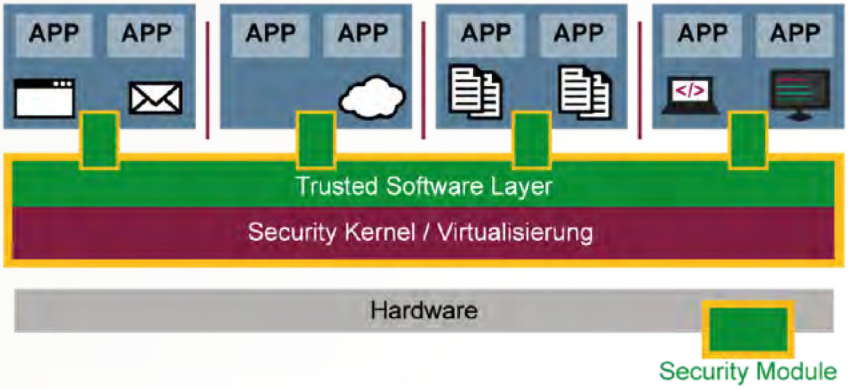

Bild 5: IT-Sicherheitsarchitektur

Durch die Virtualisierung befinden sich auftretende Fehler in Form von Schwachstellen oder Schadsoftware im Prinzip in einer virtuellen Maschine. Diese befindet sich in einem abgeschlossenen Bereich und wird mittels Isolierung von anderen virtuellen Maschinen abgegrenzt. So kann diese keine weitere virtuelle Maschine infizieren. Der IT-Sicherheitsaspekt der Modularisierung ist eine Möglichkeit, Anwendungen, die zusammengehören, in einer gemeinsamen virtuellen Maschine laufen zu lassen und Anwendungen, die getrennt sein sollen, in verschiedene virtuelle Maschinen auszulagern. IT-Sicherheitsmechanismen, wie Trusted Boot, Remote Attestation, Binding und Sealing, reduzieren zusätzlich das Risiko eines Schadens durch einen erfolgreichen Angriff auf die IT-Systeme.[7] Beispielsweise bietet die SINA-Lösung der secunet/BSI entsprechende IT-Sicherheitskomponenten, um eine geschützte Bearbeitung, Speicherung und Übertragung von vertraulichen Dokumenten zu gewährleisten.

PERSONELLE MASSNAHMEN

Die Mitarbeiter brauchen Wissen darüber, welche Unternehmenswerte zu schützen sind, welche Gefahren lauern und welche IT-Sicherheitsmaßnahmen helfen, die Risiken eines Schadens des eigenen Unternehmens zu minimieren. Dazu sollten unterschiedliche personelle Maßnahmen eingeführt werden, damit die Ziele der Mitarbeiter und Unternehmen die gleichen sind und gemeinsam für mehr Sicherheit und Vertrauenswürdigkeit gesorgt werden kann. Beispiele sind:

Sicherheitsbewusstsein schaffen (Security Awareness)

Ziel von Security Awareness ist es, die durch Mitarbeiter verursachten Gefahren für die IT-Sicherheit zu minimieren. Security Awareness soll die Mitarbeiter auch davor schützen, auf Social Hacking, Phishing-Angriffe ... hereinzufallen. In Security-Awareness-Schulungen werden zuerst die wichtigsten Verhaltensregeln im Umgang mit alltäglichen Situationen vermittelt, um Fehlverhalten vorzubeugen. Das sind zum Beispiel der sichere Umgang mit E-Mails und Passwörtern, das sichere Surfen im Internet oder die Bedrohung durch und das Verhindern von Malware.

Umgang mit (dienstlichen) Informationen klären

Besonders der Umgang mit dienstlichen Informationen stellt Arbeitnehmer im Homeoffice vor neue Herausforderungen. Auf technischer Seite steht unter anderem die Verschlüsselung und Zwei-Faktor-Authentifizierung (2FA) für den Schutz sensibler Daten zur Verfügung. Auf der personellen Seite sollten die Mitarbeiter darüber aufgeklärt werden, wie sensible Informationen auf Papier geschützt werden können. Dabei besteht für den Arbeitnehmer die Aufgabe darin, nach Beendigung der Tätigkeit oder längeren Pause im Homeoffice seinen Arbeitsplatz so zu hinterlassen, dass keine Informationen, die im Zusammenhang mit der Tätigkeit im Un-

ternehmen stehen, zugänglich sind – weder für Mitbewohner, Ehepartner, Kinder oder Freunde/Besucher.[8]

Schatten-IT unterbinden

Die Unterbindung der Schatten-IT sollte mittels Richtlinien und Aufklärung transparent gemacht werden. Unternehmen sollten Bewusstsein über die Risiken von Schatten-IT und ihrer Verwendung schaffen sowie Richtlinien implementieren, die regeln was erlaubt ist. Wenn möglich, sollten die Unternehmen eigene oder besonders sichere und vertrauenswürdige Dienste zur Verfügung stellen, damit dieses Risiko minimiert wird.

ORGANISATORISCHE MASSNAHMEN

Unter die organisatorischen Sicherheitsmaßnahmen fällt beispielsweise eine Regelung, durch die klar und transparent wird, was das Unternehmen von den Mitarbeitern erwartet. Im Folgenden ein paar Beispiele:

Erreichbarkeit von Mitarbeitern im Homeoffice

Der Informationsfluss muss in den vereinbarten Zeiten gewährleistet sein. Dafür sind Kommunikationsinfrastrukturen, wie interne Chat-Systeme, zur Aufrechterhaltung der Prozesse und Abläufe zu schaffen. Zudem muss die Erreichbarkeit des Arbeitnehmers sichergestellt sein, beispielsweise durch Listen der telefonischen Erreichbarkeit von Mitarbeitern im Homeoffice.

Vorfallreaktionen und Meldewege

Im Rahmen der organisatorischen Maßnahmen sollten Geschäftsprozesse und Richtlinien angepasst werden. Besonders relevant sind Vorfallreaktionen wie Meldewege aus dem Homeoffice bei Verlust von IT-Systemen oder mobilen Endgeräten.

Support-Prozesse

Zur Unterstützung der Arbeitnehmer im Homeoffice sollten Support-Prozesse implementiert werden. Beispielsweise sollte vorab geklärt werden, wie Mitarbeiter bei Problemen mit der IT aus dem Unternehmen unterstützt werden können.

Clean-Desk

Eine sogenannte Clean-Desk-Richtline hilft dabei, sicherzustellen, dass unternehmensbezogene Informationen nicht offen zugänglich sind und ein allgemeiner Zugriffsschutz gegen Unbefugte auf die Homeoffice-IT umgesetzt wird. Dies kann durch abschließbare Schreibtische und Rollcontainer erfolgen.[4] [8] Ferner sollte vor Beginn der Arbeit des Homeoffice definiert werden, welche Informationen außerhalb der Institution transportiert und bearbeitet werden und welche Schutzvorkehrungen dafür zu treffen sind.

ZUSAMMENFASSUNG UND AUSBLICK

Homeoffice wird auch in den folgenden Jahren eine zentrale Rolle in der modernen und digitalen Arbeitswelt einnehmen. Unternehmen müssen dafür sorgen, dass Heimarbeitsplätze sicher und vertrauenswürdig sind, um eigene Risiken und Schäden zu minimieren. Daher sollten technische, personelle und organisatorische IT-Sicherheitsmaßnahmen eingeführt und kontinuierlich verbessert werden. ■

CHRISTIAN BÖTTGER,
Student im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen. Böttger beschäftigt sich im Rahmen des Studiums mit der Sicherheit und Vertrauenswürdigkeit von Homeoffice.

NORBERT POHLMANN,
Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

Quellen/Literaturverzeichnis

[1] *Bundesamt für Sicherheit in der Informationstechnik, „bsi.bund," [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/SINA.pdf?__blob=publicationFile&v=8. [Zugriff am 26.02.2021].*

[2] *Statistisches Bundesamt, „destatis," [Online]. Available: https://www.destatis.de/DE/Themen/Arbeit/Arbeitsmarkt/Qualitaet-Arbeit/Dimension-3/home-office.html#:~:text=2019 Prozent20haben Prozent2012 Prozent2C9 Prozent20 Prozent25 Prozent20aller,Arbeitstage Prozent20von Prozent20zu Prozent20Hause Prozent20aus. [Zugriff am 15.02.2021].*

[3] *eset Deutschland GmbH, „Quo vadis, Unternehmen?," Jena, 2020.*

[4] *N. Pohlmann, „Sicheres und vertrauenswürdiges Arbeiten im Homeoffice," Gelsenkirchen, 2020.*

[5] *N. Pohlmann, „Chancen und Risiken von Smart Home," DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, 2/2021.*

[6] *C. Böttger und N. Pohlmann, „Fernkooperation mit Risiko? – Videokonferenzsystem Zoom im Sicherheitscheck," IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, Ausgabe 4/2020, August 2020, S. 60.*

[7] *N. Pohlmann, Cybersicherheit Das Lehrbuch für Architekturen, Konzepte, Prinzipien, Mechanismen und Eigenschaften, Springer Vieweg, 2019, S. 594.*

[8] *Bundesamt für Sicherheit in der Informationstechnik, „Tipps für sicheres mobiles Arbeiten," Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2020.*

[9] *M. Hertlein, „Home Office - Smart, Sicher, Effizient durch starke Nutzerauthentifizierung, remote on-boarding und elektronische Signaturen," Gelsenkirchen, 2020.*

Bild: ©Xtock - stock.adobe.com