Sechs Tipps

Arbeit im Homeoffice hat die Gefahr von Cyberangriffen erhöht – TÜV-Verband gibt Hinweise die digitale Sicherheit zu verbessern

In der fünften Corona-Welle mit der Omikron-Variante arbeitet fast jede:r vierte Beschäftigte (23 Prozent) ausschließlich im Homeoffice oder mobil. Weitere 21 Prozent geben an, dass sich bei ihnen Homeoffice und das Arbeiten im Büro abwechseln. Das hat eine Forsa-Umfrage im Auftrag des TÜV-Verbands unter 1.507 Erwerbstätigen ergeben, die vom 18. bis 23. Januar 2022 durchgeführt wurde. „Die massenhafte Arbeit im Homeoffice hat die Gefahr von Cyberangriffen erhöht", sagte Dr. Dirk Stenkamp, Präsident des TÜV-Verbands.

Mobiles Arbeiten und Homeoffice als Teil des New-Work-Konzepts stellen Arbeitgeber und Beschäftigte vor Herausforderungen bei digitaler Sicherheit. Die Risiken steigen, wenn sich privat und beruflich genutzte Infrastrukturen vermischen. Welche Rolle spielt Cybersecurity in einer digitalen und mobilen Arbeitswelt? Wie ergänzen sich Wirtschafts- und Verbraucherschutz bei New Work? Und welche Rolle kann ein IT-Sicherheitsgesetz 3.0 dabei spielen? Grafik: TÜV Verband

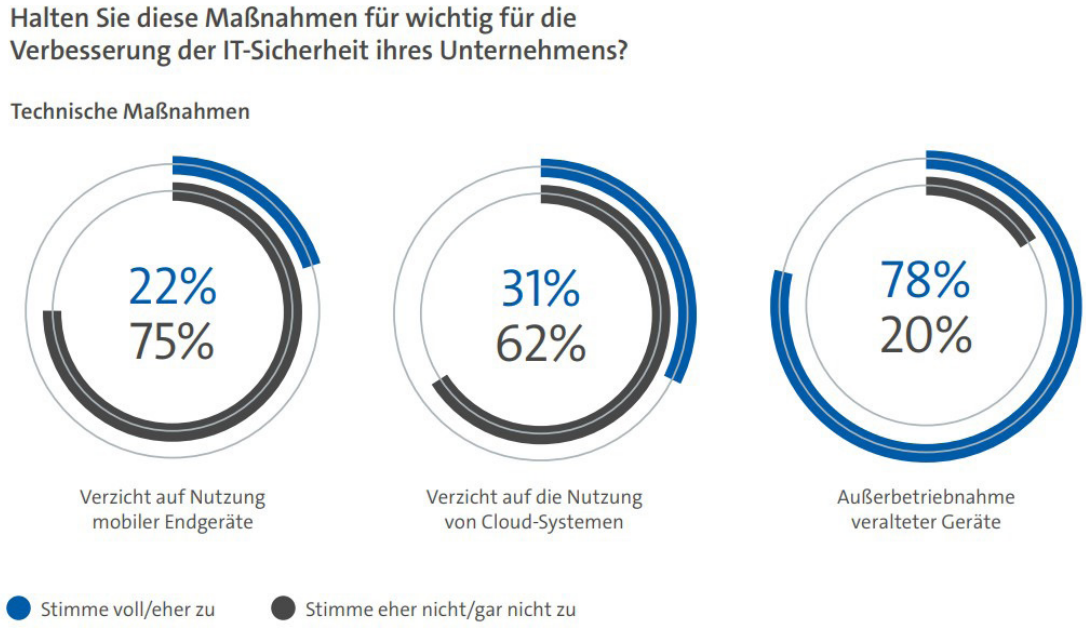
„Häufig fehlt es an Schulungen, klaren Verhaltensregeln im Fall eines IT-Angriffs oder an der notwendigen technischen Ausstattung." Laut der Umfrage berichten 14 Prozent der Erwerbstätigen, dass es in den vergangenen zwei Jahren bei ihrem Arbeitgeber zu einem oder mehreren IT-Sicherheitsvorfällen gekommen ist. In der Regel handelt es sich dabei um erfolgreiche Phishing-Angriffe oder gezielte Attacken mit Erpressungssoftware (Ransomware). 41 Prozent der befragten Arbeitnehmer:innen geben an, dass es keine Vorgaben ihres Arbeitsgebers gibt oder ihnen keine Regeln bekannt sind, wie sie sich bei einem IT-Sicherheitsvorfall verhalten sollen. „Bei erfolgreichen IT-Angriffen ist Zeit ein entscheidender Faktor, um den Schaden möglichst schnell eindämmen zu können", betonte Stenkamp. Erfolgreiche oder auch vermutete Angriffe müssten sofort gemeldet und das betroffene Gerät vorsorglich vom Internet getrennt werden, bevor weiterer Schaden entsteht.

Schulung zum Thema mobiles Arbeiten

Laut den Ergebnissen der Umfrage haben nur 38 Prozent der im Homeoffice arbeitenden Befragten an einer Schulung zum Thema mobiles Arbeiten teilgenommen. Als wichtigste Inhalte der Schulungen nennen 85

Prozent der Teilnehmenden die Erkennung von Cyberangriffen, 84 Prozent die Einhaltung des Datenschutzes beim mobilen Arbeiten und 81 Prozent das richtige Verhalten bei IT-Sicherheitsvorfällen. Aber auch Themen wie Ergonomie am Arbeitsplatz (61 Prozent) oder der Umgang mit Anwendungen wie Videokonferenz-Systemen wurden behandelt (54 Prozent). „Die Arbeit im Homeoffice stellt Arbeitgeber und Beschäftigte vor technische, organisatorische und arbeitspsychologische Herausforderungen", sagte Stenkamp. „Regelmäßige Schulungen sind ein wichtiges Mittel, um Belastungen im Homeoffice zu verringern sowie sicheres und effizientes Arbeiten zu ermöglichen."

In der Umfrage geben knapp drei von vier Befragten an (74 Prozent), dass es für die Arbeit im Homeoffice zum Thema IT-Sicherheit bestimmte Regeln ihres Arbeitgebers gibt. Davon geben 74 Prozent an, dass sie regelmäßig Software-Updates installieren sollen, 64 Prozent dürfen keine privaten USB-Sticks nutzen und bei 56 Prozent existieren Regeln oder ein Verbot für die private Nutzung von Geräten und Anwendungen.



Die Studie als PFD finden Sie hier. KLICKEN Sie einfach auf die Grafik und das PDF öffnet sich.

48 Prozent dürfen keine privaten Cloud-Dienste mit dem Computer des Arbeitgebers nutzen und bei 39 Prozent gibt es Vorgaben oder sogar ein Verbot für die Nutzung öffentlicher WLAN-Netze. Nur 8 Prozent der im Homeoffice Tätigen müssen Vorgaben für die Konfiguration des heimischen Routers befolgen. Stenkamp: „Jeder vierte Beschäftigte arbeitet im Homeoffice ohne jegliche Vorgaben des Arbeitsgebers zur IT-Sicherheit. Unternehmen und andere Arbeitgeber sind damit ein leichtes Ziel für Cyberkriminelle."

Als wichtigste Sicherheitsmaßnahmen nennen 69 Prozent der Homeoffice-Beschäftigten den Einsatz eines so genannten VPN-Clients, um eine sichere Verbindung zum Netzwerk des Arbeitsgebers herstellen zu können. 21 Prozent nutzen eine Internetbrowser-basierte Verschlüsselung. 31 Prozent nennen weitere Sicherheitsvorkehrungen wie beispielsweise Passwortschutz, Virenscanner oder Firewalls.

Der TÜV-Verband gibt Hinweise, wie Arbeitnehmer:innen die digitale Sicherheit im Homeoffice verbessern können:

- **Berufliches und Privates trennen**

  Wer mit dem Computer seines Arbeitgebers privat im Internet surft, kann sich auf diesem Weg gefährliche Schad-Software einfangen. Neben der ausschließlichen Nutzung von Geräten des Arbeitgebers für berufliche Zwecke kann es sinnvoll sein, ein eigenes WLAN-Netzwerk für die Arbeit einzurichten und Kommunikation der Geräte untereinander im Heimnetzwerk zu unterbinden.

- **Phishing-Mails erkennen und löschen**

  Vorsicht ist grundsätzlich bei allen E-Mails von unbekannten Absendern geboten. Phishing-Mails enthalten Links zu gefährlichen Webseiten mit dem Ziel, Zugangsdaten des Benutzers „abzufischen".

Zudem verschicken Cyberkriminelle massenhaft Spam-E-Mails mit Anhängen, in denen sich Schad-Software versteckt. Daher dürfen die Dateianhänge und möglichst auch die E-Mails selbst nicht geöffnet werden. Verdächtige E-Mails sollten gelöscht oder zunächst an den IT-Support des Arbeitgebers weitergeleitet werden.

- **Social Engineering als Gefahr**
  Besonders findige Cyberkriminelle greifen Organisationen gezielt an, indem sie Mitarbeiter:innen persönlich kontaktieren und täuschend echte E-Mail-Adressen verwenden. Das sollten alle Beschäftigten im Hinterkopf behalten und prüfen, ob die Absender:innen seriös sind.

- **Alle Software-Updates durchführen**

  Sowohl im Büro als auch im Homeoffice sollten Beschäftigte Software-Updates möglichst zügig durchführen. In vielen Fällen werden mit den Updates Sicherheitslücken geschlossen oder zusätzliche Sicherheitsfeatures installiert.

- **Teilnehmer:innen von Online-Meetings identifizieren**

  In größeren Online-Meetings mit Zoom, Microsoft Teams oder anderen Videokonferenz-Tools verlieren die Teilnehmenden schnell den Überblick, wer anwesend ist. Die Organisatoren des Meetings sollten darauf achten, alle Teilnehmenden persönlich zu identifizieren – entweder namentlich, per Kamera oder mit einer Vorstellungsrunde. Das ist vor allem notwendig, wenn sensible Informationen in einem Meeting geteilt werden.

- **An IT-Support wenden**

  Beschäftigte sollten die Vorgaben des Arbeitgebers und des IT-Supports beachten und keine eigenen Software-Anwendungen nutzen. Sind Mitarbeiter:innen auf Tools angewiesen, die nicht vom Arbeitgeber unterstützt werden, sollten sie dennoch den Kontakt zu ihrem IT-Support suchen und absprechen, was erlaubt ist und was nicht. Bei einem Sicherheitsvorfall sollten Beschäftigte nicht zögern und sofort die IT-Abteilung kontaktieren.

Maurice Shahd

Methodik-Hinweis: Grundlage der Angaben ist eine repräsentative Forsa-Umfrage im Auftrag des TÜV-Verbands unter 1.507 Erwerbstätigen ab 18 Jahren, die vom 18. bis 23. Januar 2022 durchgeführt wurde. Die Fragen lauteten: „Arbeiten Sie zurzeit ausschließlich oder teilweise im Home-Office bzw. mobil am Computer/Laptop?“, „Gab es in den vergangenen zwei Jahren einen oder mehrere IT-Sicherheitsvorfälle bei Ihrem Arbeitgeber?“, „Gibt es bei Ihrem Arbeitgeber Vorgaben oder Prozesse, wie sich Mitarbeiterinnen und Mitarbeiter bei einem IT-Sicherheitsvorfall verhalten sollten?“, „Gibt es für das mobile Arbeiten bzw. die Arbeit im Home-Office bestimmte Vorgaben oder Regeln zum Thema IT-Sicherheit von Ihrem Arbeitgeber?“, „Haben Sie an einer Schulung zum Thema mobiles Arbeiten bzw. Arbeiten im Home-Office teilgenommen, z. B. für die Aufklärung zum Thema IT-Sicherheit?“ Weitere Informationen unter www.tuev-verband.de/digitalisierung/cybersecurity

Über den TÜV-Verband: **Der TÜV-Verband e. V.** vertritt die politischen und fachlichen Interessen seiner Mitglieder gegenüber Politik, Verwaltung, Wirtschaft und Öffentlichkeit. Der Verband setzt sich für technische und digitale Sicherheit bei Produkten, Anlagen und Dienstleistungen durch unabhängige Prüfungen und qualifizierte Weiterbildung ein. Mit seinen Mitgliedern verfolgt der TÜV-Verband das Ziel, das hohe Niveau der technischen Sicherheit in unserer Gesellschaft zu wahren und Vertrauen für die digitale Welt zu schaffen.