Presseinformation

DEKRA gibt Tipps zum Arbeiten am PC im Home-Office

DEKRA e.V.
Konzernkommunikation
Handwerkstraße 15
D-70565 Stuttgart

www.dekra.de/presse

Einfallstor für Cyber-Kriminelle

- Nur frei gegebene Medien verwenden
- E-Mails immer in „Plain Text“ anzeigen
- Arbeitgeber müssen schulen, schulen, schulen

Die Arbeit im Home-Office kann leicht zum Einfallstor von Cyber-Kriminellen werden, warnen die IT-Spezialisten der Expertenorganisation DEKRA. Fern vom IT-Operator des Arbeitgebers öffnen sich beim Arbeiten von zuhause aus häufig Sicherheitslücken, die auch die Unternehmens-IT in Gefahr bringen können.

„Bei der Datensicherheit ist der Mensch das größte Einfallstor für Cyber-Kriminelle, das auch Technik nicht zuverlässig verschließen kann“, sagt Ingo Legler, Experte für Informationssicherheit bei DEKRA. „Aber der Mensch kann auch das größte Bollwerk sein, wenn er aufmerksam ist und weiß was er tut.“ Für Beschäftigte im Home-Office kommt dem Einhalten der Mindeststandards der IT-Sicherheit deshalb essenzielle Bedeutung zu.

Rechner beim Verlassen immer sperren

„Der Arbeitsplatz muss geeignet sein. Der Couchtisch, an dem der Rest der Familie spielt oder fernsieht, ist es nicht“, betont Legler. „Auch sollte bewusst sein, dass der Rechner zu Hause nicht so sicher ist wie im Büro.“ Also gilt: den Computer immer sperren (Windows-Symbol+L oder STRG+ALT+ENTF), wenn man den Heim-Arbeitsplatz verlässt.

Einstellungen nicht verändern

Wichtig ist auch: „Nutzen Sie nur den zugelassenen Rechner und nur die freigegebenen Zugänge, selbst wenn etwas anderes funktioniert und viel einfacher ist – für den Hacker ist es dann nämlich auch einfacher!“, so der DEKRA IT-Experte. Wichtig ist es zudem, alle Einstellungen so zu belassen, wie sie vom Firmensupport eingestellt wurde. Änderungen darf nur der Support durchführen.

Nur freigegebene Medien verwenden

Auch wenn es einfach und schnell geht, sollen Heim-Anwender Daten nie auf nicht zugelassenen Medien wie USB-Stick, HDD, SSD oder Cloud Services (Dropbox, OneDrive, Amazon Drive, iCloud) verwenden. USB-Sticks

Datum Stuttgart, 17. November 2020 / Nr. 098
Kontakt Tilman Vögele-Ebering
Telefon direkt +49.711.7861-2122
Telefax direkt +49.711.7861-742122
E-Mail tilman.voegele-ebering@dekra.com

unbekannter Herkunft, die zum Beispiel auf Tagungen oder Messen ausliegen dürfen nicht ungeprüft an den Rechner angeschlossen werden.

Sichere Passwörter verwenden

Ein kritisches Thema sind noch immer die Passwörter. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt komplexe Passwörter mit mindestens zwölf Stellen. Sie dürfen nicht aus dem Wörterbuch stammen und sollten aus einer drei-von-vier-Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. DEKRA Experte Legler: „Wichtig ist, das Passwort sofort zu ändern, wenn der Verdacht besteht, dass es geknackt wurde." Die Passwörter selbst müssen sicher aufbewahrt werden – am besten im Kopf!

E-Mail als Einfallstor für Cyber-Angriffe

Große Vorsicht ist bei Mails unbekannter Herkunft geboten. Wer unüberlegt den Anhang öffnet oder auf Links klickt, holt sich schnell Viren oder Trojaner auf den Rechner. „Bei allen nicht alltäglichen Mails muss sich der Nutzer fragen: Warum bekomme ich diese Mail?", empfiehlt DEKRA Experte Legler. Man sollte sich folgende Fragen stellen: Bin ich dort Kunde? Habe ich zeitnah etwas gekauft oder Kontakt gehabt? Was können andere mit Daten von mir anfangen? Hole ich mir sicherheitshalber IT-Hilfe?

Mails in „Plain Text" anzeigen

Am besten ist es, Mails im „Plain Text" anzuzeigen, das heißt unformatiert im reinen Textformat. Das ist nicht schön, zeigt aber verräterische Links und kleine versteckte HTML-Schnipsel, die im Hintergrund auf eine gefährliche Seite führen. Plain Text dagegen zeigt, ob der Link tatsächlich zum gewünschten Anbieter führt oder zu einer fragwürdigen Webadresse.

Vorsicht vor Social Engineering

„Vorsicht ist bei neuen Bekanntschaften zu empfehlen, die ein großes Interesse an Ihrer Arbeit zeigen – da muss man doppelt vorsichtig sein!", sagt IT-Experte Legler. Social Engineering heißt die Methode, mithilfe menschlicher Kontakte sicherheitstechnisch wichtige Daten auszuforschen.

„Arbeitgeber müssen schulen, schulen, schulen"

„Je länger das letzte Training zurückliegt, umso mehr nimmt das Bewusstsein der Mitarbeiter für IT-Sicherheit rapide ab", weiß Legler. „Arbeitgeber müssen deshalb schulen, schulen, schulen. Awareness ist das A und O."

Über DEKRA

Seit mehr als 90 Jahren arbeitet DEKRA für die Sicherheit: Aus dem 1925 in Berlin gegründeten Deutschen Kraftfahrzeug-Überwachungs-Verein e.V. ist eine der weltweit

führenden Expertenorganisationen geworden. Die DEKRA SE ist eine hundertprozentige Tochtergesellschaft des DEKRA e.V. und steuert das operative Geschäft des Konzerns. Im Jahr 2019 hat DEKRA einen Umsatz von voraussichtlich mehr als 3,4 Milliarden Euro erzielt. Fast 44.000 Mitarbeiter sind in mehr als 60 Ländern auf allen fünf Kontinenten im Einsatz. Mit qualifizierten und unabhängigen Expertendienstleistungen arbeiten sie für die Sicherheit im Verkehr, bei der Arbeit und zu Hause. Das Portfolio reicht von Fahrzeugprüfungen und Gutachten über Schadenregulierung, Industrie- und Bauprüfung, Sicherheitsberatung sowie die Prüfung und Zertifizierung von Produkten und Systemen bis zu Schulungsangeboten und Zeitarbeit. Die Vision bis zum 100. Geburtstag im Jahr 2025 lautet: DEKRA wird der globale Partner für eine sichere Welt.