Pressemeldung
August 2021

Endgeräte in Unternehmen sind das größte Einfallstor für Kriminelle

Es gibt kaum noch Unternehmen, die vor Cyberattacken verschont bleiben.

Föhren, 26.08.2021 – Cyberattacken haben in den vergangenen Jahren deutlich zugenommen. Nach einer aktuellen Studie des Digitalverbands Bitkom waren in 2020/2021 fast neun von zehn Unternehmen davon betroffen. Vor allem im Mittelstand sind IT-Sicherheitsvorfälle angestiegen. Dadurch entstehen allein in Deutschland inzwischen Schäden im Rekordwert von etwa 223 Milliarden Euro pro Jahr.

Dabei handeln Hacker oftmals aus finanziellen Gründen und versuchen erfolgreich in das Firmennetzwerk einzudringen, um gezielt Daten zu stehlen oder auch Organisationsabläufe zu sabotieren. Erpressungsvorfälle sind die Folge.
Auch die Forschung in Instituten oder Unternehmen, sieht sich zunehmend der Wirtschaftsspionage und Konkurrenzausspähung ausgesetzt, die durch totalitäre Staaten oder durch Mitbewerber stattfinden. Langjährige Entwicklungsergebnisse, Prototypen oder Kundendaten werden abgegriffen, für eigene Zwecke genutzt oder weiter veräußert.

Verdachtsindikatoren erkennen und Präventionsmaßnahmen durchführen
Kriminelle setzen beispielsweise auf die Neugier oder ein achtloses Handeln der Endanwender. Ein geöffneter und infizierter E-Mail-Anhang oder der Besuch einer schadhaften Webseite genügt bereits, um Hackern den Zugang in das Unternehmensnetzwerk zu ermöglichen. Seit Anbeginn der Pandemie und der resultierenden Möglichkeit des Arbeitens aus dem Homeoffice heraus, konnte ein Zuwachs derartiger IT-Sicherheitsvorfälle verzeichnet werden.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) rät zu Grundregeln, die Anwender im täglichen Arbeitsumfeld beachten sollten. Es gilt die Devise: „Erst denken, dann klicken“.

1. Bewertung eingehender E-Mails. Vor dem Öffnen sollte geprüft werden, ob der Absender bekannt und mit dem Warenabsender der Mail identisch ist.
2. Äußerste Vorsicht bei E-Mails mit Anhängen. Denn Anhänge können täuschend echt dargestellt sein.
3. Im Zweifelsfall nachfragen. Oftmals reicht ein kurzer Anruf bei dem bekannten Absender, um sich die Korrektheit der E-Mail und Dateianhangs bestätigen zu lassen.
4. Bei Verdachtsfällen informieren. Verdächtige E-Mails sollten nicht weitergeleitet werden. Es empfiehlt sich die interne IT telefonisch zu informieren, um die weitere Vorgehensweise abzusprechen.

In jedem Unternehmen müssen klare Verhaltensregeln greifen, um alle Mitarbeiter für die Gefahren von Cyberkriminalität und Industriespionage zu sensibilisieren. Denn ein potenzielles Risiko geht auch direkt von Innentätern aus.
Im Kooperationsverbundprojekt der Institute Max-Planck sowie Fraunhofer wurde das Projekt WISKOS ins Leben gerufen, was die Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa genauer untersuchte. Im Ergebnis wurden hilfreiche Handlungsleitfäden erstellt, die Unternehmen bei der Prävention unterstützen. **(siehe Fußnote[1] „Kostenfreie Handlungsleitfäden“)**.

Unterstützung erhalten Mitarbeiter durch technische Maßnahmen, für die sich die interne IT verantwortlich zeigt. Im Einsatz befindliche Tools sind in der Lage, Auffälligkeiten zu erkennen und bspw. bei größeren Datentransfers eine Warnmeldung auszulösen.
Mit dem Einsatz von weiteren Security-Lösungen können zudem verdächtige E-Mail-Eingänge erkannt, gefiltert und eliminiert werden. Die Endpunktsicherheit der Clients ist gewährleistet. Ihre Daten bleiben geschützt und der Geschäftsbetrieb wird nicht gestört.

Eine der marktführenden Sicherheitslösungen für die Absicherung von Endgeräten ist „Microsoft Defender for Endpoint“, was auch unabhängige Analysten wie Gartner bestätigen.

Kostenfreier Impuls-Vortrag für IT-Verantwortliche aus dem Bereich Endpunktsicherheit/Client-Management oder Virenschutz
Um über den Schutz und möglicher Abwehrszenarien zu informieren, veranstaltet die IT-HAUS GmbH am **31.08.2021 um 12:30 Uhr einen 30-minütigen Webcast zum Thema „Endpunktsicherheit“.**
Im Schwerpunkt wird die die Microsoft Defender-Plattform betrachtet, die sich nicht nur an Windows-User richtet, sondern auch für Mac, Android und iOS zur Verfügung steht.
Gerade für Unternehmen, die bereits Microsoft Office 365 nutzen, bieten sich weiterführende Möglichkeiten, den eigenen Kosten- und Administrationsaufwand zu reduzieren.
Interessierte IT-Verantwortliche aus Unternehmen können sich kostenfrei unter Microsoft Defender for Endpoint - IT-HAUS Website informieren und registrieren.

[1] ***Kostenfreie Handlungsleitfäden für Unternehmen und Wissenschaftsorganisationen***
Unter www.wiskos.de erhalten Unternehmen und Wissenschaftsorganisationen gezielte Handlungsleitfäden, die bei der Aufklärung und Prävention unterstützen.

BILDDATEN
Adobe Stock

PRESSE-KONTAKT
IT-HAUS GmbH | Marketing | Europa-Allee 26/28 | D-54343 Föhren
Tel.: +49 6502 9208-0 | E-Mail: marketing@it-haus.com

MANAGEMENT SUMMARY

Die IT-HAUS GmbH ist eines der TOP 25 IT-Systemhäuser in Deutschland. Kunden aus dem B2B-Geschäftsumfeld partizipieren von umfangreichen Full-Service-Konzepten und -Lösungen, um die IT sowie deren anhängende Prozesse – im Hinblick auf die unternehmensweite Wachstumsstrategie – zukunftsfähig auszurichten. Diese reichen von Managed Print Konzepten über Cloud-Lösungen bis hin zu Digital Signage Anwendungen am Point-of-Sale. Dabei stellen proaktive technische Services eine essenzielle Ausrichtung im Hinblick auf Industrie 4.0 und die digitale Transformation dar. Durch ein flächendeckend globales Netzwerk ermöglicht IT-HAUS seinen Kunden die Integration weltweiter Beschaffungsstrategien und Kostenvorteile durch optimierte Prozesse. Auch in 2020 wurde die IT-HAUS GmbH zu einem der Besten Systemhäusern gekürt und 2021 wiederholt als Top-Managed-Service-Provider ausgezeichnet.