Veröffentlicht auf Presseportal Schweiz - Presse und Medienmitteilungen (https://www.presseportal-schweiz.ch)

19.09. 2016

Fachkräftemangel bei IT-Profis gefährdet IT-Sicherheit in Unternehmen

Von PPS

Bild Rechte
Robert Half

Checkliste: Wie Unternehmen ein wirksames IT-Sicherheitsprogramm aufbauen

(Zürich)(PPS) **Laut der Global State of Information Security® Survey 2016 der Unternehmensberatung PwC hat im Jahr 2015 die Anzahl der Datendiebstähle und Bedrohungen durch Wirtschaftsspionage oder Sabotage weltweit um 38 % zugenommen. Diese Gefahr wird durch fehlende IT-Sicherheitsexperten zukünftig noch verstärkt, wie eine Befragung von 960 CIOs und CTOs in acht Ländern [1] durch den spezialisierten Personaldienstleister Robert Half Technology ergab.**

Mehr als drei Viertel der Technologieverantwortlichen (78 %) glauben, dass es in den kommenden fünf Jahren aufgrund des Fachkräftemangels in der IT-Sicherheit zu einem Anstieg bei Sicherheitsbedrohungen für Unternehmen kommt.

„Die Gefahren durch Cyber-Angriffe werden immer grösser. Doch technische Lösungen allein reichen nicht aus, um sich dagegen zu schützen,“ so Sven Hennige, Senior Managing Director Central Europe & The Netherlands bei Robert Half Technology. *„Unternehmen sind auf qualifizierte IT-Sicherheitsexperten angewiesen, die für eine systematische Absicherung und die Umsetzung einer IT-Sicherheitsstrategie sorgen. Unter Einhaltung gesetzlicher Regelungen und unternehmensinterner Compliance-Vorgaben können IT-Experten etwa Sicherheitsupdates einspielen oder Authentifizierungsprozesse für den Zugang zum Unternehmensnetzwerk implementieren.“*

Grösstes IT-Sicherheitsrisiko: Datenmissbrauch

Das grösste IT-Sicherheitsrisiko für Organisationen geht nach Einschätzung der befragten CIOs und CTOs in den kommenden fünf Jahren von Datenmissbrauch aus (57 %), gefolgt von Cyber-Kriminalität wie Datendiebstahl oder Erpressung (52 %). An dritter Stelle steht Wirtschaftsspionage durch Spy- oder Ransomware (46 %).

Robert Half Technology hat CIOs und CTOs weltweit gefragt: ***Welche der folgenden IT-Sicherheitsrisiken werden für Ihre Organisation in den kommenden fünf Jahren die grösste Relevanz haben?***

Datenmissbrauch/Datenintegrität

57 %

Cyberkriminalität (Betrug, Erpressung, Datendiebstahl)

52 %

Spionage/Spyware/Ransomware (Wirtschaftsspionage)

46 %

Mangelnde(s) Wissen/Sicherheitskompetenz von Mitarbeitern

35 %

Angriffe von innen (z. B. Gefährdung von Mitarbeitern oder internen Akteuren)

27 %

Abhängigkeit von Dritten

12 %

Quelle: Robert Half, Arbeitsmarktstudie 2016, Befragte: 960 CIOs und CTOs in acht Ländern

„Durch die fortschreitende Digitalisierung und die komplexere Vernetzung von Prozessen steigt nicht nur die Wettbewerbsfähigkeit eines Unternehmens, sondern auch das Risiko, Opfer von Cyber-Kriminalität zu werden," erläutert Sven Hennige. „*Unternehmen müssen daher nicht nur betriebliche Prozesse und Daten absichern, sondern auch externe Schnittstellen mit Lieferanten oder Vertragspartnern auf IT-Risiken wie mangelnden Datenschutz prüfen. Diese IT-Sicherheit gilt es fortlaufend zu kontrollieren und auf dem aktuellen Stand zu halten, denn die Professionalisierung der virtuellen Angreifer entwickelt sich ebenfalls weiter.*"

Robert Half Technology gibt Tipps, wie Unternehmen ein wirksames IT-Sicherheitsprogramm entwickeln und implementieren können:

1. Seien Sie aktiv:
Entwickeln Sie vorausschauende Richtlinien, um sich gegen Cyber-Angriffe zu schützen. Stellen Sie sicher, dass die erforderlichen Massnahmen ergriffen werden, um effizient auf Sicherheitsverstösse reagieren zu können.

2. Nutzen Sie Big Data:
Nutzen Sie mithilfe von geeigneten Tools alle verfügbaren Daten, um herauszufinden, welche Risiken zu- oder abnehmen und welche Bereiche zusätzliche Sicherheitsmassnahmen erfordern.

3. Etablieren Sie unternehmensweite Prozesse für Ihre IT-Sicherheit:
Führen Sie gründliche Risiko- und Bedrohungsanalysen durch und evaluieren Sie bestehende Prozesse und Systeme immer wieder, um Risiken zu minimieren. Auch das Risikomanagement der Lieferanten und Partner ist zu beachten.

4. Sichern Sie sich die erforderlichen Kompetenzen:
Investieren Sie mit umfassenden Fortbildungsmassnahmen in vorhandene IT-Fachkräfte oder ergänzen Sie Ihr Team mit neuen Mitarbeitern, um sich die erforderliche Expertise zu sichern. Berücksichtigen Sie auch die Möglichkeit, mit externen IT-Experten oder Beratern zusammenzuarbeiten.

5. Binden Sie alle mit ein:
Stärken Sie das Risikobewusstsein aller Mitarbeiter in Bezug auf den Umgang mit E-Mails, Social Media und vertraulichen Informationen. Anstatt Mitarbeiter lediglich in einer E-Mail über aktuelle Risiken zu informieren, fördern Sie regelmässige Schulungen zu Sicherheitsrichtlinien und zur Unternehmenspraxis.

Über die Studie:

Für die Studie wurden 960 CIOs und CTOs in Australien, Brasilien, Frankreich, Deutschland, Hongkong, Singapur, Grossbritannien und Japan befragt. Die Erhebung wurde im Rahmen der Arbeitsmarktstudie von einem internationalen unabhängigen Meinungsforschungsinstitut im Auftrag von Robert Half Technology, dem spezialisierten Personaldienstleister für Fach- und Führungskräfte im IT-Bereich, durchgeführt. Weitere Studienergebnisse finden Sie unter roberthalf.ch/presse.

Für Pressegespräche steht Ihnen Sven Hennige, Senior Managing Director bei Robert Half, gerne zur Verfügung. Zur Terminvereinbarung kontaktieren Sie bitte Christina Holl, Tel. +49 89 5454 260 22 oder christina.holl@roberthalf.de bzw. Gabriela Mair, Tel. +43 1 4085794 oder g.mair@procomm.biz.

Die Pressemitteilung können Sie unter roberthalf.ch/presse abrufen. Dort finden Sie auch Informationen zu früheren Studien.

[1] Australien, Brasilien, Frankreich, Deutschland, Hongkong, Singapur, Grossbritannien, Japan

Pressekontakt:

Robert Half
Herzog-Wilhelm-Straße 26
80331 München
Christina Holl
T: 49 (0)89 545 426 022
E: christina.holl@roberthalf.de

Kategorie
IT & Software & Neue Medien
