– Presseinformation der Controlware GmbH –

Mit Controlware in fünf Schritten zum ganzheitlichen Risikomanagement

Dietzenbach, 11. Dezember 2018 – Controlware, renommierter deutscher Systemintegrator und Managed Service Provider, hat einen kompakten Leitfaden für die Durchführung von Risikoanalysen entwickelt. Unternehmen schaffen so in fünf einfachen Schritten die Voraussetzungen für ein nachhaltiges Informationssicherheitsmanagement und stellen die Weichen für eine bereichsübergreifende Risikominimierung.

Cyberattacken auf Daten und Systeme der Unternehmen nehmen rasant zu – und bedeuten in Zeiten strenger Compliance-Vorgaben und hoher Bußgelder ein erhebliches finanzielles Risiko. Hinzu kommt, dass ein erfolgreicher Angriff oder Datendiebstahl auch den Ruf des betroffenen Unternehmens nachhaltig schädigt. IT-Abteilungen sind daher mehr denn je auf ganzheitliche Sicherheitskonzepte angewiesen. Voraussetzung dafür ist aber zunächst ein unternehmensweites Risikomanagement. Georg Basse, Senior Consultant Information Security bei Controlware, erklärt: „Wer wirkungsvolle technische und organisatorische Maßnahmen im Bereich IT-Security treffen will, muss zuerst einmal alle potenziellen Risiken kennen. Das ist mit Blick auf die Komplexität moderner IT-Infrastrukturen aber alles andere als einfach. Daher haben wir mithilfe der Best Practices aus unseren erfolgreichen Kundenprojekten einen Leitfaden entwickelt, der beim Start ins Risikomanagement unterstützt."

Mit folgenden fünf Schritten schaffen IT-Teams die Voraussetzungen für eine belastbare, unternehmensweite Risikobewertung:

1. Identifizieren Sie die Zielobjekte

Erfassen und klassifizieren Sie im ersten Schritt alle relevanten Zielobjekte. Hierzu gehören nicht nur die Anwendungen, IT-Systeme und Netzkomponenten, sondern auch Gebäude, Räume, Mitarbeiter oder Kommunikationsverbindungen. In der Regel existieren Inventarlisten oder Netzpläne, die bereits viele der benötigten Informationen enthalten. Ziehen Sie solche Unterlagen zurate, um Mehrarbeit und Zeit zu sparen.

2. Analysieren Sie Schwachstellen der Ziele

Legen Sie gemeinsam mit Ihren Kollegen fest, welche Schwachstellen die jeweiligen Zielobjekte aufweisen. Achten Sie darauf, Mitarbeiter unterschiedlicher Unternehmensbereiche einzubeziehen, um eine holistische Sichtweise sicherzustellen: Der IT-Verantwortliche wird

Sitz: Controlware GmbH Kommunikationssysteme ▪ Waldstraße 92 ▪ 63128 Dietzenbach ▪ GERMANY
Tel. +49 6074 858-00 ▪ Fax +49 6074 858-108 ▪ info@controlware.de ▪ www.controlware.de
Registergericht Offenbach a.M. ▪ HRB Nr. 6431 ▪ USt-IdNr. DE 113 539 225 ▪ Steuernummer 3523035235
Geschäftsführer (CEO) Bernd Schwefing

wahrscheinlich uneingeschränkte Zutritte zu Serverräumen oder fehlende Software-Updates als mögliche Schwachstellen nennen, während der Betriebsrat vielleicht eher an unverschlüsselt abgelegte Mitarbeiterdaten denkt. Halten Sie auch fest, wie wahrscheinlich die von Ihnen festgestellten Schwachstellen auftreten. Hierfür genügt ein einfaches Schema, etwa in Kategorien wie „möglich“, „theoretisch“ oder „bekannt“.

3. Analysieren Sie potenzielle Bedrohungen

Losgelöst von den Schwachstellen sollten Sie sich im nächsten Schritt einen Überblick über potenzielle Bedrohungen verschaffen. Hierzu zählen beispielsweise externe Angriffe mit Ransomware oder Denial-of-Service-Attacken, aber auch verärgerte Mitarbeiter, die Ihre Hard- oder Software manipulieren. Versuchen Sie hierbei, die Eintrittswahrscheinlichkeiten der Bedrohungen möglichst akkurat zu beziffern. Angesichts der komplexen und dynamischen Bedrohungslandschaft hat es sich in dieser Phase sehr bewährt, externe Consultants hinzuzuziehen.

4. Formulieren Sie mögliche Gefährdungen

Korrelieren Sie Bedrohungen und Schwachstellen und leiten Sie daraus konkrete Gefahren für Ihr Unternehmen ab. Diese können zum Beispiel lauten: „Infiltrieren des Netzwerks (Zielobjekt) über ungepatchte Mitarbeiter-PCs (Schwachstelle) mithilfe eines Office-Exploits (Bedrohung)“. Aufgrund der hohen Zahl und der Vielfalt der IT-Komponenten werden sich in diesem Schritt zwangsläufig sehr viele potenzielle Gefahren ergeben. Um den Überblick zu behalten, sollten Sie gleiche Gefährdungen in Gruppen zusammenfassen. So reduzieren Sie den Aufwand der Risikoanalyse, ohne den Detaillierungsgrad zu senken.

5. Führen Sie eine Risikoanalyse durch

Im letzten Schritt – der eigentlichen Risikoanalyse – setzen Sie die Eintrittswahrscheinlichkeiten der Gefährdungen mit der zu erwartenden Schadenshöhe in Korrelation. Die so erhaltenen Werte zeigen, mit welcher Priorität die einzelnen Risiken anzugehen sind, und helfen Ihnen fundiert zu entscheiden, ob Sie sofort handeln müssen, einen Dritten mit der Behandlung beauftragen sollten oder vielleicht sogar mit dem Risiko leben können. Kommunizieren Sie die ermittelten Risiken in jedem Fall an die Stake Holder und Entscheider Ihres Unternehmens und überwachen Sie kontinuierlich, ob die getroffenen Maßnahmen wirksam sind.

„Unternehmen sollten das Risikomanagement nicht auf die leichte Schulter nehmen. Wer zum ersten Mal eine Risikoanalyse durchführt, übersieht leicht gefährliche Schwachstellen oder Bedrohungen – oder ist mit der Vielzahl zu evaluierender Gefährdungen schlicht überfordert“,

Sitz: Controlware GmbH Kommunikationssysteme ▪ Waldstraße 92 ▪ 63128 Dietzenbach ▪ GERMANY
Tel. +49 6074 858-00 ▪ Fax +49 6074 858-108 ▪ info@controlware.de ▪ www.controlware.de
Registergericht Offenbach a.M. ▪ HRB Nr. 6431 ▪ USt-IdNr. DE 113 539 225 ▪ Steuernummer 3523035235
Geschäftsführer (CEO) Bernd Schwefing

warnt Georg Basse. „Daher ist es ratsam, bereits zu Beginn des Projekts kompetente externe Partner hinzuzuziehen. Aufsetzend auf deren Projekterfahrung lassen sich viele Fallstricke vermeiden und gängige Risiken wesentlich besser einschätzen."

5.028 Zeichen (inkl. Leerzeichen).

Über Controlware GmbH

Die Controlware GmbH, Dietzenbach, ist einer der führenden unabhängigen Systemintegratoren und Managed Service Provider in Deutschland. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden. Das Portfolio erstreckt sich von der Beratung und Planung über Installation und Wartung bis hin zu Management, Überwachung und Betrieb von Kundeninfrastrukturen durch das firmeneigene ISO 27001-zertifizierte Customer Service Center. Zentrale Geschäftsfelder der Controlware sind die Bereiche Network Solutions, Collaboration, Information Security, Application Delivery, Data Center & Cloud sowie IT-Management. Controlware arbeitet eng mit national und international führenden Herstellern zusammen und verfügt bei den meisten dieser Partner über den höchsten Zertifizierungsgrad. Das rund 760 Mitarbeiter starke Unternehmen unterhält ein flächendeckendes Vertriebs- und Servicenetz mit 16 Standorten in DACH. Im Bereich der Nachwuchsförderung kooperiert Controlware mit fünf renommierten deutschen Hochschulen und betreut durchgehend um die 50 Auszubildende und Studenten. Zu den Unternehmen der Controlware Gruppe zählen die Controlware GmbH, die ExperTeach GmbH, die Networkers AG und die Productware GmbH.

Pressekontakt:
Stefanie Zender
Controlware GmbH
Tel.: +49 6074 858-246
Fax: +49 6074 858-220
e-mail: stefanie.zender@controlware.de
www.controlware.de (Homepage)

Belegexemplare bitte an:
Michal Vitkovsky
H zwo B Kommunikations GmbH
Tel.: +49 9131 81281-25
Fax: +49 9131 81281-28
e-mail: michal.vitkovsky@h-zwo-b.de
www.h-zwo-b.de (Homepage)