IT-Sicherheit einfach managen!

Der digitale Wandel schafft neue Arbeitsmethoden, Bedürfnisse und Herausforderungen in Unternehmen. Um mit der Geschwindigkeit der digitalen Transformationen mitzuhalten, ist eine umfassende und flexible Security-Lösung unvermeidbar. Unser Security-Experte klärt über die neuen Herausforderungen und Chancen auf.

In den letzten Jahren hat die Digitalisierung in Unternehmen entscheidend Fahrt aufgenommen. Traditionelle Arbeitsweisen wurden Großteils von modernen Arbeitsweisen ersetzt. Diese zeichnen sich vor allem dadurch aus, dass der persönliche Arbeitsplatz unabhängig von Ort und Gerät gewählt werden kann, die Zusammenarbeit übergreifend stattfindet und Informationen auch von remote zugänglich sind.

Welche Konsequenzen hat diese Entwicklung auf die IT-Sicherheit in einem Unternehmen?
Simon Kofler: Dieser Umschwung stellt die IT-Sicherheit in Unternehmen vor neue Herausforderungen: Einerseits erschwert der Zugriff von beliebigen Orten und Geräten aus die Abgrenzung einer Unternehmensumgebung, die es zu schützen gilt. Andererseits macht der fehlende direkte Kontakt zwischen Mitarbeitern diese zu einem bedeutsamen Angriffspunkt.

Diesen Risiken gilt es mit neuen Sicherheitsmethoden entgegenzuwirken. Wie kann man eine solche, effiziente Sicherheits-Lösung aufbauen?
Simon Kofler: Eine ideale Sicherheits-Lösung umfasst drei Bereiche: den Faktor Mensch, die Technik und die Organisation von Prozessen und Richtlinien. Um eine optimale Lösung zu finden, muss ein Unternehmen diese kritischen Bereiche genau analysieren und eine individuelle Strategie entwickeln, die zu internen und externen Gegebenheiten passt. Zuletzt muss sich ein Unternehmen laufend mit implementierten Strategien und Systemen auseinandersetzten und gegebenenfalls Anpassungen vornehmen.

Was kann man sich unter einer solchen Strategie vorstellen?
Simon Kofler: In erster Linie sind die gewählten Technologien entscheidend, vor allem im Hinblick auf die Entwicklung von flexiblen Arbeitsmethoden. Deshalb sollten Tools und Anwendungen von überall aus für Mitarbeiter zugänglich gemacht werden, beispielsweise durch die Verlagerung in eine Cloud. Da der IT-Umgebung nun keine Grenzen mehr gesetzt sind, muss auch das Sicherheitskonzept neu definiert werden. Eine Möglichkeit ist dabei der Einsatz des Zero-Trust Modells. Dabei wird jeder Zugriffsversuch als nicht vertrauenswürdig eingestuft und mehrfach überprüft, zum Beispiel durch Multi-Faktor-Authentifizierung und Überprüfung des Endgerätes.
Mindestens genauso wichtig sind und bleiben die Mitarbeiter des Unternehmens. Ziel ist es, jeden Mitarbeiter das Wissen zu vermitteln, um Angriffsversuche zu erkennen und bewusst darauf zu reagieren. Durch gezielte Security Awareness Trainings kann ein nachhaltiges Sicherheits- und Risikobewusstsein im Unternehmen erreicht werden.

Ist die Lösung nun im Unternehmen umgesetzt, muss sie laufend kontrolliert und angepasst werden. Wie kann ein Unternehmen diese zeit- und ressourcenaufwändige Herausforderung optimal meistern?
Simon Kofler: KONVERTO bietet mit dem Managed Service „Security Operation Center" eine professionelle Lösung. Dabei werden Unternehmen von der Beratung, zur Entwicklung einer individuellen Lösung bis hin zu fortlaufender Überwachung unterstützt. Das SOC schützt die IT-Infrastruktur und Daten des Unternehmens vor internen und externen Gefahren. Die kontinuierliche Überwachung und Analyse von Sicherheits-Experten begrenzt das Risiko von Cyberattacken entscheidend, ermöglicht es Bedrohungen frühzeitig zu erkennen und sofort darauf zu reagieren.

Gestire la sicurezza IT in modo semplice!

La trasformazione digitale crea nuovi metodi di lavoro, esigenze e sfide nelle aziende. Per tenere il passo con la velocità delle trasformazioni digitali, una soluzione di sicurezza completa e flessibile è indispensabile. Il nostro esperto di sicurezza spiega le nuove sfide e opportunità.

Negli ultimi anni, la digitalizzazione nelle aziende si è velocizzata in modo decisivo. I tradizionali metodi di lavoro sono stati in gran parte sostituiti dai più moderni. Questi sono caratterizzati soprattutto dal fatto che il posto di lavoro personale può essere scelto indipendentemente dal luogo e dal dispositivo, la collaborazione avviene in modo trasversale e si può accedere alle informazioni anche a distanza.

Quali sono le conseguenze di questo sviluppo per la sicurezza informatica in un'azienda?
Simon Kofler: Questo cambiamento pone nuove sfide per la sicurezza informatica nelle aziende: Da un lato, l'accesso da qualsiasi luogo e dispositivo rende più difficile delimitare un ambiente aziendale che deve essere protetto. D'altra parte, la mancanza di contatto diretto tra i dipendenti li rende un punto di attacco pericoloso.

Questi rischi devono essere contrastati con nuovi metodi di sicurezza. Come si può costruire una soluzione di sicurezza adatta?
Simon Kofler: Una soluzione di sicurezza ideale comprende tre aree: il fattore umano, la tecnologia e l'organizzazione dei processi e delle linee guida. Per trovare una soluzione ottimale, un'azienda deve analizzare queste aree critiche in dettaglio e sviluppare una strategia individuale che si adatti alle circostanze interne ed esterne. Infine, un'azienda deve esaminare continuamente le strategie e i sistemi che sono stati implementati e apportare modifiche se necessario.

Cosa si intende per una simile strategia?
Simon Kofler: Innanzitutto, la scelta delle tecnologie è fondamentale, soprattutto per quanto riguarda lo sviluppo di metodi di lavoro flessibili. Gli strumenti e le applicazioni devono essere resi accessibili ai dipendenti da qualsiasi luogo, per esempio trasferendoli su un cloud. Considerando poi, che l'ambiente IT non è più limitato, anche il concetto di sicurezza deve essere ridefinito. Una possibilità è quella di utilizzare il modello zero-trust. Ogni tentativo di accesso viene classificato come non affidabile e sarà controllato più volte, per esempio attraverso l'autenticazione a più fattori e il controllo del dispositivo finale.
I dipendenti dell'azienda sono e rimarranno almeno altrettanto importanti. L'obiettivo è quello di fornire ad ogni dipendente le conoscenze per riconoscere i tentativi di attacco e reagire ad essi in modo consapevole. Attraverso corsi di Security Awareness, è possibile raggiungere una consapevolezza sostenibile della sicurezza e dei rischi nell'azienda.

Una volta che la soluzione è stata implementata in azienda, deve essere continuamente monitorata e adattata. Come può un'azienda gestire in modo ottimale questa sfida che richiede tempo e risorse?
Simon Kofler: KONVERTO offre una soluzione professionale con il suo managed service "Security Operation Center". Con questo servizio, le aziende sono assistite dalla consulenza, fino allo sviluppo di una soluzione individuale e al monitoraggio continuo. Il SOC protegge l'infrastruttura IT e i dati dell'azienda contro le minacce interne ed esterne. Il monitoraggio e l'analisi continua da parte degli esperti di sicurezza limita decisamente il rischio di attacchi informatici, permette di riconoscere le minacce in una fase iniziale e di reagire immediatamente.