Cyberangriffe: Wie Wiesbadener Unternehmen besser vorbereitet sind

Erfahren Sie, wie Unternehmen Cybersecurity-Vorfälle effektiv meistern und Schäden minimieren können – mit proaktiven Strategien und Notfallplänen.

Wiesbaden (ots)

Cyberangriffe sind heutzutage eine weit verbreitete Bedrohung für Unternehmen aller Größen und Branchen. Die Gefahr, die von Hackern und Ransomware ausgeht, ist nicht mehr auf große Konzerne beschränkt, sondern betrifft auch kleine und mittlere Unternehmen. Dies wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt, das betont, dass diese Cyberangriffe eine der größten Herausforderungen für die deutsche Wirtschaft darstellen.

Besonders die steigende Vernetzung von IT-Systemen und das Wachstum digitaler Infrastrukturen schaffen neue und lukrative Angriffsflächen. Für Unternehmen wird es immer wichtiger, sich nicht nur auf Lösungen zur Verhinderung auf Cyberangriffe zu konzentrieren, sondern auch darauf, wie man die Folgen solcher Vorfälle effektiver managen kann. Die aktuelle Realität erfordert eine grundlegende Änderung in der Denkweise – die Annahme, dass ein Angriff nur eine Frage der Zeit ist.

Vorbereitung ist der Schlüssel

Im Gespräch mit Sven Ulke, Senior Manager DFIR bei der SVA System Vertrieb Alexander GmbH, wird deutlich, dass es entscheidend ist, gut vorbereitet zu sein, um auf Cybervorfälle

zu reagieren. Oft werden Sicherheitsvorfälle nicht schnell genug erkannt, was dazu führt, dass Unternehmen unvorbereitet in einen Notfall geraten. Es reicht nicht aus, einfach das letzte Backup zu verwenden, ohne sicherzustellen, dass die Hintertür für Angreifer geschlossen wird. Wenn nicht alle notwendigen Schritte unternommen werden, kann das Problem schnell zurückkehren, was die Notwendigkeit eines fundierten Incident Response Plans unterstreicht.

Ein effektiver Notfallplan sollte sowohl die Analyse der Situation als auch die Festlegung notwendiger Schutzmaßnahmen beinhalten. Zudem ist es wichtig, einen Krisenstab innerhalb des Unternehmens zu benennen, der im Ernstfall schnelle und koordinierte Entscheidungen treffen kann. Solche Pläne sollten regelmäßig geprobt werden, um Stress und Chaos im Fall des Falles zu minimieren und sicherzustellen, dass alle Mitarbeiter ihre Rolle kennen.

Doch wie Sven Ulke erklärt, gibt es keine universelle Vorlage für einen erfolgreichen Incident Response Plan. Jedes Unternehmen hat seine eigenen spezifischen Anforderungen und Herausforderungen, was bedeutet, dass Anpassungsfähigkeit und proaktive Kommunikation mit Fachleuten unerlässlich sind. Der regelmäßige Austausch mit Dienstleistern wie SVA hilft dabei, potenzielle Gefahren frühzeitig zu erkennen und adäquate Vorkehrungen zu treffen.

Individuelle Lösungen für individuelle Herausforderungen

Die Risikobewertung eines Unternehmens ist entscheidend, um herauszufinden, welche IT-Systeme am stärksten gefährdet sind und wie man die wichtigsten Vermögenswerte bestmöglich schützt. Oftmals wird dies jedoch als herausfordernd empfunden. Die Business Impact Analyse der SVA unterstützt die Unternehmen dabei, ihre kritischen Systeme zu identifizieren und geeignete Maßnahmen zu priorisieren.

Zusätzlich müssen die empfohlenen Maßnahmen auch umsetzbar sein. SVA bietet maßgeschneiderte technologische und organisatorische Lösungen entsprechend den spezifischen Ressourcen und Bedürfnissen ihrer Kunden. Die enge regionale Zusammenarbeit ermöglicht es dem Unternehmen, schnell einen umfassenden Überblick über die Unternehmensstruktur zu gewinnen und die besten Vorgehensweisen zu empfehlen.

Ein wichtiger Aspekt ist die 24/7 Notfall-Hotline der SVA, die Hilfe in akuten Notfällen bietet und gleichzeitig die Möglichkeit eröffnet, bei schwerwiegenden Vorfällen direkt vor Ort zu assistieren. Das Team hat zudem die Kompetenz, komplette Netzwerke oder Serversysteme wiederherzustellen und benötigt dafür eine breite Expertise, die durch viele Herstellerpartnerschaften unterstützt wird.

Nicht zu vergessen sind die regulatorischen Anforderungen, die Unternehmen heute erfüllen müssen. Unterstützung bei der Umsetzung der Datenschutz-Grundverordnung der EU, sowie der Erfüllung der neuen IT-Sicherheitsgesetze, ist ebenfalls Bestandteil deren Services. Die richtige Vorbereitung und Unterstützung im Cybersecurity-Bereich sind somit nicht nur vorteilhaft, sondern für viele Unternehmen essentiell geworden, um den Herausforderungen der digitalen Welt standzuhalten.

Details