Success Story

biwac webagentur

Ransomware Resilience stärken

Seit 25 Jahren begleitet die biwac webagentur ihre Kundinnen und Kunden zum digitalen Erfolg. Wer – wie die junge Firma aus Solothurn – den digitalen Raum bespielt, ist nicht nur durch technische oder kundenspezifische Herausforderungen gefordert. Cyberkriminelle treiben ihr Unwesen und lassen das Damoklesschwert «Ransomware» furchteinflössend über grossen und kleinen Unternehmen schweben. Das wirft die Frage auf, wie es denn um die Stärke der eigenen Widerstandskraft gegen Ransomware-Attacken bestellt ist. Der Workshop Ransomware Resilience der Swiss Infosec AG liefert Antworten und Handlungsempfehlungen.

Wer sich im Bereich von Websites und E-Commerce einen Namen gemacht hat, versteht sein Handwerk. Und wer seit 25 Jahren im Geschäft ist, weiss, was es heisst, sich immer wieder neuen Herausforderungen zu stellen und anzupassen. Auf die biwac webagentur treffen beide Aussagen zu. Das kleine, feine Unternehmen bietet im Bereich Websites umfassende Dienstleistungen an: von der Beratung/Konzeption, über Interaction Design, Programmierung und Entwicklung bis hin zu Schulung und Support und weiterer ergänzender Dienstleistungen. Auf dem anderen Standbein – E-Commerce – konzipieren, programmieren und promoten die Kreativen aus Solothurn Magento-Shops.

Damoklesschwert Ransomware

Ransomware (Schadprogramme, die Computer sperren oder Daten verschlüsseln), ist zu einer veritablen Seuche geworden. Die Frage ist deshalb nicht, ob ein Unternehmen angegriffen wird, sondern wann und wie oft. Eine gute Abwehr gegen Cyberattacken, idealerweise gepaart mit wirkungsvoller Business Continuity, ist deshalb unumgänglich. Die biwac webagentur hat sich vor dem Hintergrund der Bedrohungslage durch Cyberangriffe zum Ziel gesetzt, ihre Ransomware-Resilience zu überprüfen und zu optimieren. Eine solche Überprüfung steht im Zentrum des halbtägigen Workshops Ransomware Resilience der Swiss Infosec AG, für den sich die biwac webagentur entschieden hat.

Punkt für Punkt zu mehr Klarheit

Die Grundlage des Workshops bildet eine Checkliste, die auf Erfahrungen aus der Praxis, Standards wie den CIS Controls v8 und Security Best Practice-Empfehlungen basiert und sich von der Struktur her am NIST Cybersecurity-Framework orientiert. Der Inhalt des Workshops wird dynamisch gestaltet und orientiert sich an den zentralen Herausforderungen der Organisation, welche je nach Unternehmensgrösse, Branche und Unternehmenskultur sehr unterschiedlich sein können. Als roter Faden dienen das NIST Cybersecurity-Framework und die von der Swiss Infosec erstellte Checkliste. Die Checkliste stellt unterstützend sicher, dass alle wichtigen Themen bei der Vorbereitung auf mögliche Ransomware-Angriffe berücksichtigt werden. Dieses Vorgehen stellt sicher, dass keine Aspekte vergessen werden und die Ergebnisse aussagekräftig in den Schlussbericht einfliessen.

Die Vorteile liegen auf der Hand

Ziel des Workshops, der in der Regel digital durchgeführt wird, ist es, die Cybergesundheit eines Unternehmens möglichst umfassend und strukturiert abzuklären und konkrete, klar priorisierte Handlungsempfehlungen abzuleiten. Diese werden in einem Bericht zusammengestellt. Der Ransomware Resilience Workshop bietet ein hohes Kosten-/Nutzen-Verhältnis, da die Vorbereitung einer Organisation auf mögliche Angriffe innert eines Nachmittags gesamtheitlich besprochen wird. Dies gilt insbesondere dann, wenn wie bei der biwac webagentur, Wille und Offenheit vorhanden sind, engagiert mitzudiskutieren und Handlungsempfehlungen konsequent umzusetzen.

Fabian Bill
Leitung E-Commerce, biwac webagentur

«Durch die unabhängige Aussensicht der Spezialisten der Swiss Infosec AG haben wir wichtige Erkenntnisse zur Cybergesundheit unseres Unternehmens gewonnen. Unsere Resilienz gegen Ransomware-Attacken können wir durch die vorgeschlagenen Handlungsempfehlungen massgeblich stärken.»

★★★★★

biwac webagentur