Wer (Cyber-)Sicherheit nicht ernst nimmt, bekommt mit Sicherheit Probleme

Im Interview informiert der Geschäftsführer der Infotech EDV-Systeme GmbH, Martin Mallinger, zur Lage der Cybersecurity in österreichischen Unternehmen. Außerdem spricht er über häufige Herausforderungen und darüber, wie sich diese meistern lassen.

FOTO: INFOTECH EDV-SYSTEME GMBH

Ing. Martin Mallinger, MSc
Geschäftsführer

Wie cybersicher sind österreichische Unternehmen?
Große Unternehmen sind bei der Cybersecurity häufig weiter als KMUs, immer häufiger haben sie eigene Expert:innenteams. Oft sind Unternehmen schon mit grundlegenden Sicherheitsmaßnahmen überfordert (Patch Management, Backup, Benutzer:innenverwaltung und Multi-Faktor-Authentication, MFA). Das macht sie angreifbar.

Schätzen hiesige Unternehmer:innen digitale Souveränität?
Den meisten EU-Unternehmen ist ihre große Abhängigkeit von US-amerikanischen Unternehmen (noch) nicht bewusst. Zwänge die US-Regierung US-Unternehmen mit Sanktionen dazu, EU-Unternehmen den Zugriff auf ihre Cloud-Services zu verbieten, hätten viele EU-Unternehmen keinen Zugriff mehr auf E-Mails, Telefonie und Unternehmensdaten. Deshalb raten wir unseren Kund:innen, sich Gedanken über Exit- und Notfallszenarien zu machen, wenn sie cloudbasierte Services aus den USA nutzen. Als Anbieter souveräner Cloud-Services sichern wir Daten von Unternehmen in selbstbetriebenen, lokalen Clouds.

Wichtig: Für ein Mehr an Souveränität muss man nicht mit dem Schwierigsten, wie der Ablöse von MS-365-Services starten. Für viele einfache Anwendungen gibt es Alternativen – auch von regionalen Cloud-Anbietern, wie z. B. den my.bizcloud-Services (https://www.mybizcloud.at) aus unserem Haus.

Was sind die drei größten Schwachstellen von Unternehmen?
1. Ganz weit vorne ist die Annahme, dass das eigene Unternehmen für Angreifende uninteressant ist, weil es nichts zu holen gibt.
2. Es wird oft angenommen, dass IT-Sicherheit nur ein Kosten- und nicht auch ein Erfolgsfaktor ist.
3. Die steigende Komplexität der IT-Systemlandschaft ist schwer zu schützen.

Mit der NIS2-Richtlinie hat Europa eine EU-weite Vorgabe, um Cybersecurity zu schaffen. Ist das eine Herausforderung für Österreichs Unternehmen?
NIS2 ist vielen ein Begriff. Leider werden die Anforderungen meist negativ betrachtet, obwohl die Maßnahmen Unternehmen schützen und auf etablierten internationalen Standards (ISO/IEC 27001, 27002) beruhen. Zudem berücksichtigt NIS2 Größe und Möglichkeiten der Unternehmen. Das Besondere an der Entwicklung der nationalen Umsetzungen ist, dass viel Expert:innenwissen eingeflossen ist. Etwas unglücklich ist, dass es die letzte Regierung nicht geschafft hat, das Gesetz zu verabschieden. Das verwirrt und verunsichert Unternehmen. Viele bereits initiierte NIS2-Projekte liegen deshalb auf Eis.

Viele Unternehmen stecken noch zu viel Energie in Argumentation und Auswegsuche, um nicht unter NIS2 zu fallen – es gibt sogar Ideen zum Umstrukturieren der Gesellschaften. Davon ist klar abzuraten. Ihre Energie sollten Unternehmen lieber in eine vernünftige Umsetzung investieren.

Die größten Kritikpunkte an NIS2 sind die Feststellung der Betroffenheit (Fällt mein Unternehmen unter NIS2?) und die konzernweite/länderübergreifende Umsetzung.

Haben Sie ein Beispiel für die Umsetzung einer NIS2 Maßnahme?
Die NIS2 wird bei der Netzwerksegmentierung sehr konkret: Netze sind demnach gemäß der Risikobewertung funktional/logisch zu trennen und kritische Systeme in besonders gesicherten Zonen unterzubringen. Beide Schutzmaßnahmen sind seit Langem Best Practice – und werden dennoch von vielen Unternehmen nicht umgesetzt. Wir bieten hierfür mit unserem Partner Zero Networks moderne Lösungen an, die tatsächlich nicht nur Netzbereiche, sondern einzelne Geräte voneinander segmentieren können, und zwar auf automatisierte Art und Weise. Zudem ermöglichen wir, dass jede Verbindung, egal von welchem Nutzer, Anwendung, Protokoll oder Asset mit einer MFA (Multi Factor Authentication) versehen werden kann.

NIS2 fordert Unternehmen auch zur Notfallvorsorge auf: Kommen die Unternehmen dem nach?
Unternehmen müssen wissen, wie sich Ausfälle einzelner Systeme auf den Geschäftsbetrieb auswirken. Ein Großteil des Schadens lässt sich häufig mit einfachen Maßnahmen deutlich senken. Für verbleibende, nicht verhinderbare Ausfälle braucht es Notfallpläne. Und die sollten unbedingt auch geübt werden. Wir machen mit Kund:innen regelmäßig Disaster-Recovery-Tests. Die Testergebnisse dokumentieren wir, sodass sie als erster Notfallplan dienen können. Wichtig: Im Notfall müssen die Notfallpläne – unabhängig von den eigenen Systemen – verfügbar sein! ■

Lesen Sie mehr unter
infotech.at