IT-Sicherheit ist Chefsache

Die Fachtagung zum Thema Datenschutz und Informationssicherheit macht deutlich, dass nicht nur Datenschutzbeauftragte in sozialen Organsiationen allerhand zu tun haben.

Von Ina Füllkrug

Mit rund 50 Teilnehmerinnen und Teilnehmer startete die erste Fachtagung zum Thema „Datenschutz und Informationssicherheit in Sozialwirtschaft und Non-Profit-Organisationen“ in Paderborn. Fünf Jahre Datenschutz-Grundverordnung (DSGVO) nahm das Beratungsunternehmen Althammer & Kill zum Anlass, aufzuzeigen, wie die Anforderungen in Sachen Cloud, KI und Cyber-Security in der Praxis wirksam gestaltet werden können.

Einsatz von KI-Systemen, Cybersecurity-Attacken und Datenpannen oder die Nutzung von Cloud-Diensten aus unsicheren Drittstaaten: Verantwortliche in Sachen Datenschutz und Informationssicherheit haben allerhand zu tun, heißt es bei der Tagung. Selbst bei den „Basics“ seien auch nach ein paar Jahren „Datenschutz-Routine“ noch viele Fragen offen, wenn man sich Berechtigungsstrukturen, Löschkonzepte und andere Themen ansehe. „Um uns vor Cyber-Angriffen zu schützen, werden wir Sicherheit in Zukunft viel gründlicher umsetzen müssen“, stellt Thomas Althammer fest. So geben denn auch 13 externe und interne Expertert:innen in ihren Vorträgen wertvolle Impulse.

Zur Begrifflichkeit sei erläutert, dass es sich beim Datenschutz um personenbezogene Daten handelt, bei der IT-Sicherheit um den Schutz der IT und bei der Informationssicherheit um den Schutz aller Informationen in der Organisation. Um letzteres geht es im Workshop „Informationssicherheit“ und darum, kritische Geschäftsprozesse zu schützen. „Das sind Prozesse, die dem Unternehmen Geld bringen“, stellt Rodney Wiedemann, Berater für Datenschutz und IT-Sicherheit, klar. Er zeigt auf, warum das Thema Risikomanagement in Unternehmen so wichtig ist. „Denken Sie in worst case- Szenarien. Wenn Sie es jetzt denken, sparen Sie später Geld“, betont er.

Im Rahmen eines Business Continuity Management sollten die potenziellen Bedrohungen ermittelt und vorbeugend Strategien, Prozesse sowie Maßnahmen entwickelt werden, mit denen die Geschäftsfähigkeit eines Betriebs oder einer Organisation im Ernstfall sichergestellt werden kann.

Dafür empfiehlt er, eine Business Impact Analyse durchzuführen. Hierbei handele es sich um eine strukturierte Untersuchung mit dem Ziel, (zeit-) kritische Geschäftsprozesse und Ressourcen zu identifizieren. Es werden potenzielle Ausfälle ermittelt und in Szenarien dargestellt bzw. durchgespielt. Ganz entscheidend sei dabei die Schnelligkeit, in der bei Ausfällen oder Cyber-Angriffen gehandelt werde, so der Experte.

Schutzziele seien Vertraulichkeit, Integrität und Verfügbarkeit. Unterteilt werde in Schutzbedarfsfeststellung, Schutzkategorien und Schadensszenarien.

Risikomanagement befasse sich primär mit dem Risiko, der Schwachstelle und der Bedrohung, die immer da sei und zur Gefährdung werden könne. Die qualitative Risikoanalyse beleuchte dabei die Kosten eines Ausfalls. Die quantitative Risikoanalyse bezeichne die Bewertung der Szenarien und Einschätzung der Bedrohung durch Experten.

Thomas Althammer (li.), Geschäftsführer, und Niels Kill, Berater für Datenschutz und IT-Sicherheit, sind sich einig, dass Sicherheit in Zukunft gründlicher umgesetzt werden sollte. Foto: Ina Füllkrug

Zur Messung der Maßnahmen seien Kennzahlen optimal, so Wiedemann.

Risikomanagement sei ein kontinuierlicher Prozess und bedürfe der ständigen Überprüfung. „Risiken ändern sich und das erfordert neue Maßnahmen“, sagt Wiedemann.

Risikomanagement sei ein Managementprozess, da habe die IT-Abteilung nicht die Alleinverantwortung. Und betont schließlich noch einmal: „Sicherheit ist ein Marathon, kein Spurt.“

> **„Datensicherheit ist ein Marathon, kein Spurt.“**
>
> Rodney Wiedemann, Berater für Datenschutz und IT-Sicherheit

Hinterfragen schafft einen guten Schutz: „95 Prozent der Cyber-Angriffe werden durch menschliche Fehler erst möglich, weiß Maximilian Klose, Berater für Datenschutz und Cloud- & Cyber-Security. der sich bei Althammer & Kill auf die Security Awareness spezialisiert hat – also auf das Sicherheits-Bewusstsein aufseiten der Mitarbeitenden. Er simuliert Phishing-Attacken im Auftrag von Unternehmen, um an den Reaktionen der Mitarbeitenden aufzuzeigen, wie es um das Sicherheits-Bewusstsein bestellt ist. „Schaffen Sie ein Verständnis bei den Mitarbeitenden, denken Sie in verschiedenen Risikoschichten und implementieren Sie Security Awareness ganzheitlich“, rät Klose den Teilnehmenden – zumeist Datenschutzbeauftragte in sozialen Organisationen. Zum Schutz vor Cyber-Angriffen empfiehlt er folgende Maßnahmen:

- Den Blick schärfen, genau hinschauen – also etwa keinen fremden USB-Stick einfach so in den PC stecken.
- Vorsicht gegenüber Unbekannten
- Interne Strukturen aktiv nutzen
- Eine positive Fehlerkultur schaffen
- In den Dialog gehen

Auch das im Juli in Kraft getretene **Hinweisgeberschutz-Gesetz** steht auf der Agenda der Tagung, das laut Niels Kill „eingeschlagen hat wie eine Bombe“. Hierzu erläutert Christian Klande, Berater für Datenschutz und Compliance, zunächst, dass jede Organisation laut Legalitätspflicht die Einhaltung rechtlicher Vorgaben sicherstellen müsse. „Liegt ein Selektionsverschulden, ein Anweisungsverschulden oder ein Überwachungsverschulden vor, dann wird die Organisation in die Pflicht genommen“, so Klande.

Die Geschäftsführung habe ein Compliance Management System einzuführen, das alle Werkzeuge und Prozesse umfasse, mit denen ein Unternehmen sicherstelle, dass es sich an Regeln und Gesetze halte. Das beinhalte sowohl außerbetriebliche Vorgaben der Aufsichtsbehörden und Gesetze, als auch interne Weisungen und Verordnungen sowie rechtsverbindliche und ethische Regeln.

Info: althammer-kill.de