

[CLOUD](#)[DATACENTER](#)[INFRASTRUKTUR](#)[Home](#) > [Sicherheit](#)

Zertifiziertes ISMS als Wettbewerbsvorteil

🕒 25. August 2020



Die meisten kritischen und schützenswerten Informationen werden in Unternehmen mittels IT verarbeitet, gespeichert und abgerufen. Um den Schutz dieser Informationen zu gewährleisten, sind verschiedene technische und organisatorische Maßnahmen erforderlich. Doch IT- und

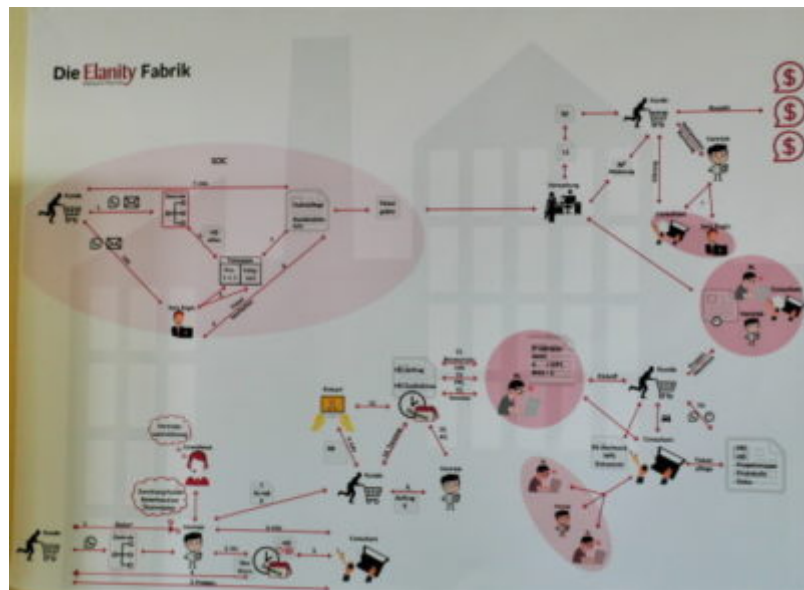
Informationssicherheit sind nicht nur einfach theoretische Anforderungen, die es zu erfüllen gilt; sie sind inzwischen entscheidend für den Geschäftserfolg eines Unternehmens. Das weiß auch Elan: Das Systemhaus unterstützt seine Kunden bei der Umsetzung von IT-Projekten und hat sich nun selbst dazu entschieden, ein softwarebasiertes Informationssicherheitsmanagementsystem (ISMS) einzuführen.



Die Elanity Network Partner GmbH steht ihren Kunden für die Planung, Beschaffung, Konfiguration und den Betrieb ihrer IT-Infrastruktur zur Seite. Daher wissen die Experten nur allzu gut, wie wichtig eine individuell zugeschnittene IT-Sicherheitsstrategie sowie angemessene IT-Lösungen in der aktuellen Bedrohungslage für Unternehmen sind. Cyberattacken nehmen stetig zu, und die Angriffsmethoden werden immer versierter. Daher sind Schäden durch Cyberangriffe mittlerweile für jedes Unternehmen – unabhängig von der Branche und Größe – eine ernstzunehmende Gefahr.

Drei Gründe für ein zertifiziertes ISMS

Zahlreiche Beispiele der letzten Jahre haben gezeigt, dass erfolgreiche Cyberangriffe



existenzgefährdende Folgen haben können. Fallen IT-Systeme über mehrere Tage aus, steht in vielen Unternehmen der gesamte Betrieb still. Insbesondere in der Industrie sind darüber hinaus auch Partner in der Lieferkette betroffen. Aus diesem Grund schützen sich immer mehr Firmen mit einer Cyberversicherung und benötigen hierfür einen Nachweis ihrer Partner oder Dienstleister, dass sie über die nötigen Zertifizierungen verfügen.

Als Systemhaus hat Elanity natürlich tiefe Einblicke in die Strukturen seiner Kunden und Zugriff auf wichtige Daten. „Nicht nur die von uns eingesetzten Lösungen, sondern auch wir selbst als Unternehmen müssen stets die aktuellen Sicherheitsstandards erfüllen. Daher liegt es in unserer Verantwortung, die von uns verarbeiteten Informationen bestmöglich zu schützen“, sagt Peter Schröder, Geschäftsführer von Elanity. „Genau aus diesem Grund sind einige unserer Kunden, die sich gerade im Prozess der ISO-Zertifizierung befinden, an uns herangetreten. Sie haben uns informiert, dass sie uns künftig nur beauftragen dürfen, wenn wir ISO-zertifiziert sind.“

Um allen erforderlichen Anforderungen gerecht zu werden, müssen Prozesse im Rahmen einer ISO-Zertifizierung nachweisbar definiert werden. Daher suchte

Elanity nach einer angemessenen Lösung mit einfachem, strukturiertem Aufbau, um langfristig weniger Aufwand in der Datenpflege zu haben. Bei der Recherche stand unter anderem die Umsetzung mit Word, Excel und Sharepoint zur Debatte. Hier zeigten sich jedoch schon bei der Evaluierung schnell erste Schwachstellen, weshalb sich die Projektverantwortlichen bei Elanity gegen diese Umsetzungsmöglichkeit entschieden. „Unser Wunsch war es, eine Datenbasis zu haben, die dann auch für die Verwaltung von Themen wie DSGVO und Notfallhandbuch etc. zur Verfügung steht“, sagt Peter Schröder. „Als Partner von Contechnet waren wir schon mit der Vorgehensweise aus den Softwarelösungen für IT-Notfallplanung und Datenschutz vertraut. Daher entschieden wir uns für die Umsetzung mit der ISMS-Software ‘INDITOR ISO‘“

Von Word und Excel zum softwarebasierten ISMS

Ein prozessorientiertes ISMS einzuführen und zu pflegen ist nur bei gewissen Branchen oder ab bestimmten Unternehmensgrößen gesetzlich gefordert. Obwohl für Elanity diese Anforderungen nicht offiziell gelten, wollte das Unternehmen Transparenz über seine IT-Landschaft schaffen.

Als Contechnet-Vertriebspartner integriert Elanity bei seinen Kunden „INDART Professional“, die Software für IT-Notfallplanung. Dadurch konnten sie die Installation weitestgehend eigenständig umsetzen und wurden in manchen Punkten von den Consultants des Softwareherstellers unterstützt. So erfolgte beispielsweise eine Anbindung an Sharepoint für die Dokumentenlenkung und an den Mailserver für den Versand von Aufgaben. „Die Installation lief weitestgehend problemlos ab“, sagt Peter Schröder. „Es gab lediglich eine Fehlermeldung beim Zugriff auf die Sharepoint-Dokumentenbibliotheken, die uns nicht erklärlich war. Hier haben wir den Support per E-Mail informiert, und dieser hat dann zügig und zielgerichtet geholfen.“

Nach der Installation begann der sukzessive Aufbau des Managementsystems. „Für uns war es zunächst ein Unterschied, dass wir bestimmte Teile eben nicht mit Excel und Word abarbeiten, wie es andere Unternehmen tun, mit denen wir die Zertifizierung angehen. Das hat anfänglich ein wenig irritiert, da man Themen nicht 1:1 gemeinsam erarbeiten konnte“, sagt Peter Schröder. „Doch schon jetzt merken wir, dass die Software eine klarere Struktur vorgibt und viele Dinge übersichtlicher sind, da nicht so viele Office-Dokumente verwendet werden, die sich gegenseitig referenzieren.“

Drei Lösungen mit einer Datenbasis

In der Software wurden die Projektverantwortlichen Schritt für Schritt durch die einzelnen relevanten Themen geleitet. Es galt, zunächst die für sich relevanten Anforderungen und Maßnahmen aus der ISO/IEC 27001 zu bestimmen und sie im Anforderungskatalog zu definieren. Um diesen Schritt zu vereinfachen, ist der



Katalog in der Lösung um Umsetzungstipps und Hilfestellungen ergänzt. Die nächste Aufgabe bestand darin, einen Überblick über die vorhandene Infrastruktur des Unternehmens zu schaffen. „Schon an diesem Punkt haben wir den für uns mitunter wichtigsten Vorteil erkannt: Die Softwarelösungen der Contechnet-Suite nutzen eine gemeinsame Datenbasis, wodurch sich diverse Synergien ergeben. Wir haben zuvor schon für unser Unternehmen ein Notfallhandbuch mithilfe der entsprechenden Contechnet-Softwarelösung erstellt und damit sozusagen die Vorarbeit geleistet.“ Denn durch die Verknüpfung der Software war im Assetmanagement der ISMS-Software bereits die Infrastruktur des Unternehmens abgebildet. Auf diese Weise konnte Elanity in kurzer Zeit Prozesse, Personal und ca. 100 Objekte anlegen, darunter Server, Storage, Computer, mobile Geräte aber auch Anwendungen und Informationen.

ISMS-Software als Unterstützung im Arbeitsalltag

Wie auch Elanitys Erfahrung aus der täglichen Praxis zeigt, sollte nicht nur die gesetzliche Anforderung ein Grund sein, sich für die Einführung eines softwarebasierten ISMS zu entscheiden. Nach dem vollständigen Aufbau des Managementsystems integrierte das Unternehmen die Lösung in die täglichen Arbeitsprozesse des Informationssicherheitsbeauftragten sowie der Verwaltung und der Geschäftsführung. „Neben der transparenten Darstellung und der Verknüpfung der einzelnen Assets überzeugt uns vor allem auch das integrierte Aufgabenmanagement. Was sonst einen deutlich höheren manuellen Aufwand und stärkere Disziplin der verantwortlichen Mitarbeiter erfordert hätte, können wir nun übersichtlich und zentral in der Software verwalten“, sagt Peter Schröder.

Aktuell befindet sich Elanity im Prozess der ersten Zertifizierung. Um weiter vom Zusammenspiel der Suite zu profitieren, plant das Unternehmen den Einsatz zu vertiefen und die Datenschutz-Lösung „INPRIVE“ des Softwareherstellers Contechnet einzuführen.

Info: Die Elanity Network Partner GmbH hat ihren Hauptsitz in Hannover. Darüber hinaus verfügt das Unternehmen über weitere Standorte in Hamburg und Uelzen. Ein Team von etwa 35 Mitarbeitern unterstützt Kunden in allen Belangen rund um ihre IT-Infrastruktur. Auf Basis einer mehr als 20-jährigen Erfahrung berät, plant und setzt Elanity spezifische IT-Lösungen bei seinen Kunden um.

The logo for Elanity Network Partner features the word "Elanity" in a large, bold, red serif font. Below it, the words "Network Partner" are written in a smaller, black, sans-serif font.

Von Samira Liebscher, freie Journalistin

INFO:

WEITERE NEWS, INTERVIEWS, ARTIKEL,
KOMMENTARE, VIDEOS, BACKGROUNDER VON CONTECHNET

KLICK



Tags: [Assetmanagement](#) [CISO](#) [Contechnet](#) [Cyberdefense](#) [Cybersecurity](#).
[Cyberversicherung](#) [Datenschutz](#) [DSGVO](#) [Elanity](#).
[Informationssicherheitsmanagementsystem](#) [ISMS](#) [IT-Notfallplanung](#) [IT-Security](#).
[IT-Sicherheit](#) [Notfallhandbuch](#) [Notfallplan](#) [Systemhaus](#)

 SHARE ON FACEBOOK SHARE ON TWITTER SHARE ON PINTEREST SHARE ON LINKEDIN SHARE ON TUMBLR SHARE ON EMAIL

Weitere interessante Beiträge

