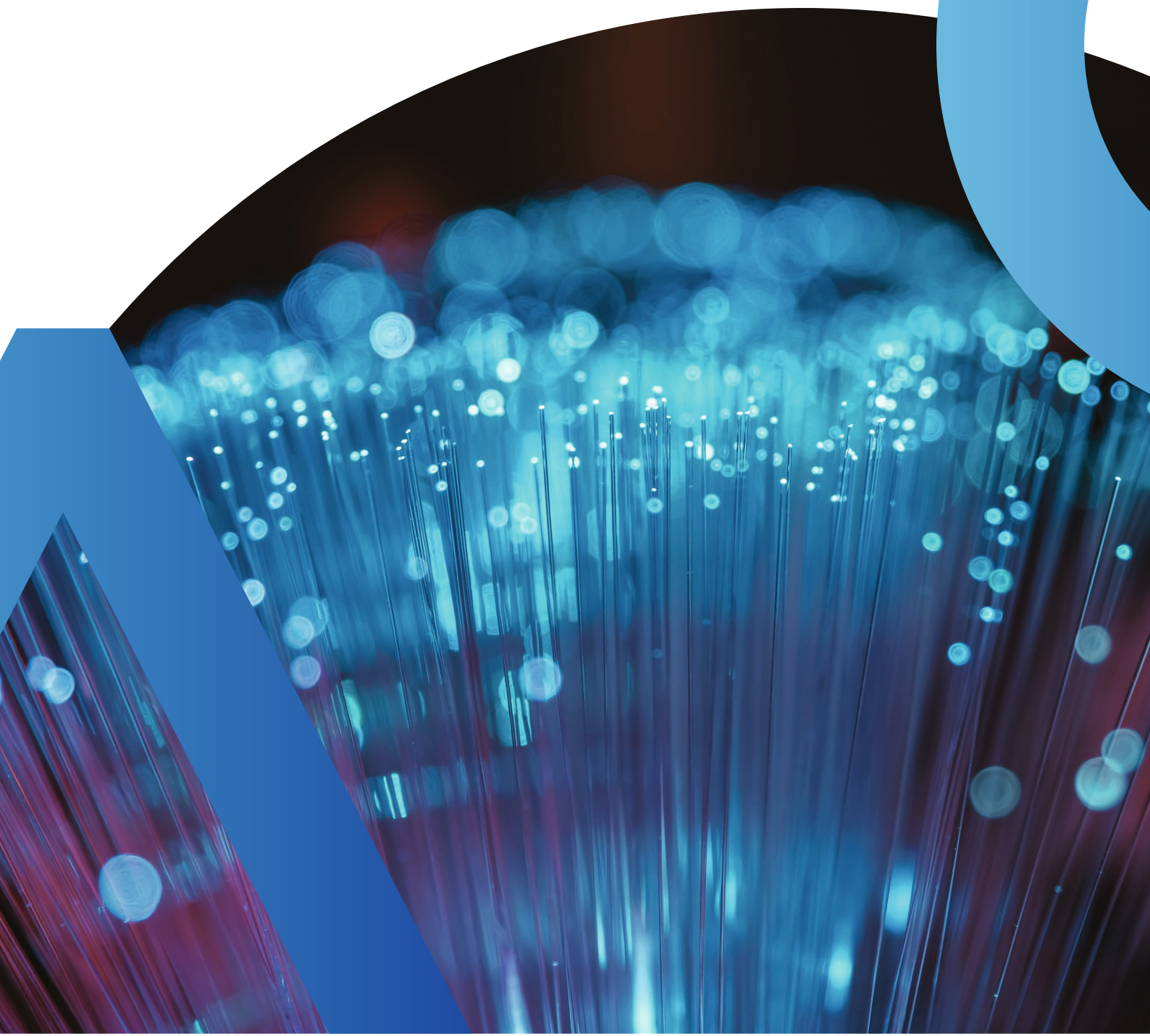
ALLGEIER secion

Anwenderbericht

Stadtwerke Tuttlingen – IT-Sicherheitsüberprüfungen unterstützen Einhaltung der ISO 27001



Gegen den unsichtbaren Gegner im (Energie-)Netz

Autorin: Samira Liebscher, freie Journalistin

Der Mitarbeiter schaltet wie jeden Morgen seinen PC an und entdeckt im überfüllten Posteingang eine E-Mail seiner IT-Abteilung. In dieser informiert ein Kollege über das neu verfügbare Intranetportal, in dem die Mitarbeiter ab sofort aktuelle News und Informationen aus dem Unternehmen erhalten. Ohne lange zu überlegen, klickt der Mitarbeiter auf den Link – und wird so bereits Opfer einer Hackerattacke. Sein Glück: Es handelt sich um eine fingierte Phishing-Kampagne. Aufgrund der wachsenden IT-Sicherheitsbedrohungen aus dem Netz haben sich die Verantwortlichen der Stadtwerke Tuttlingen dazu entschlossen, die Awareness ihrer Mitarbeiter und auch die informationstechnischen Systeme durch einen externen IT Security Spezialisten überprüfen zu lassen.

Als Energieversorger tragen die Stadtwerke Tuttlingen eine große Verantwortung für das staatliche Gemeinwesen. Ein Ausfall des Betriebs würde erhebliche Versorgungsengpässe und andere weitreichende Folgen nach sich ziehen. Gemäß Verordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zählen sie daher zu den Kritischen Infrastrukturen (KRITIS). Als diese sind sie dazu verpflichtet, ihre informationstechnischen Systeme, die für den Betrieb des Versorgungsunternehmens maßgeblich sind, „angemessen“ abzusichern. Dazu zählen nicht nur entsprechende technische Maßnahmen, sondern auch regelmäßige Überprüfungen auf eventuell vorhandene IT-Schwachstellen.

„Wir sind uns der enormen Bedeutung von IT- und Informationssicherheit bewusst und achten deshalb stark auf eine hohe Sicherheit, sowohl bei unseren Systemen als auch hinsichtlich der Awareness unserer Mitarbeiter“, sagt Florian Müller, IT-Sicherheitsbeauftragter der Stadtwerke Tuttlingen. Bereits bei der Implementierung von neuen Systemen und Geräten spielt die IT-Sicherheit eine große Rolle; so prüft das IT-Team beispielsweise regelmäßig die Konfigurationen der einzelnen Geräte im Netzwerk.

Die organisatorische Sicherheit gewährleisteten die Stadtwerke Tuttlingen schließlich mit der Einführung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001.

stadtwerke tuttlingen gmbh

Der lokale Energieversorger beliefert die Bewohner sowie Industrie- und Gewerbekunden der Stadt Tuttlingen seit 1889 mit Strom, Gas, Wärme, Wasser und kümmert sich um Schmutz- und Regenwasserentsorgung. Zudem unterstützen die Stadtwerke Tuttlingen Bauherren bei der Planung von Hausanschlüssen. Insgesamt beschäftigt die Organisation inzwischen über 160 Mitarbeiter.

Aber auch hier ist es mit einer einmaligen Zertifizierung nicht getan. Es gilt, die Maßnahmen, Abläufe und Handlungsverpflichtungen, die das ISMS festlegt, in die Unternehmenskultur zu integrieren und im Alltag zu leben. Um sich selbst sowie die IT- und Informationssicherheit auf den Prüfstand zu stellen, entschieden sich die Verantwortlichen daher, das IT-Netzwerk und die Mitarbeiter mit IT-Sicherheitsüberprüfungen durch einen externen Dienstleister unter die Lupe nehmen zu lassen.

„Wir haben uns verschiedene Dienstleister angeschaut und uns schließlich für die Allgeier secion GmbH als fachlich kompetenten Projektpartner entschieden, da uns die Expertise sowie das Preis-Leistungs-Verhältnis überzeugt hat“, beschreibt Florian Müller das Auswahlverfahren. Nach der gemeinsamen Betrachtung der Anforderungen entschieden sich die IT-Verantwortlichen der Stadtwerke Tuttlingen für einen Penetrationstest im Rahmen eines White Box-Audits sowie für eine individuelle Phishing-Kampagne. Das Ziel dieser Überprüfungen war es, alle vorhandenen Schwachstellen in der Infrastruktur sowie Wege für den unbemerkten Zugriff auf das Netzwerk und sensible Daten zu identifizieren.

Sicherheitsanalyse aus Angreiferperspektive

Nach einem automatischen Schwachstellenscan, der unter anderem erreichbare Dienste und offene Ports berücksichtigt, agierten die IT-Sicherheitsexperten in einer manuellen Schwachstellenanalyse aus der Sicht typischer Angreiferprofile. Auf diese Weise überprüften sie beispielsweise, welche Möglichkeiten sich einem externen Angreifer bieten, der vorab sicherheitsrelevante Informationen über die Stadtwerke Tuttlingen aus öffentlich verfügbaren Datenquellen, wie sozialen Netzwerken, RIPE, Shodan usw., gesammelt hat. Bereits diese Informationen können ihm dabei behilflich sein, sich Zugriff auf Dienste, Daten und Applikationen des Energieversorgers zu verschaffen. Zuletzt kontrollierten die IT-Sicherheitsexperten natürlich auch, ob die öffentlich erreichbaren Web-Applikationen der Stadtwerke Tuttlingen Schwachstellen aufweisen.

Nach der remote durchgeführten Überprüfung wurde eine detaillierte Bewertung vorgenommen. Dabei ging es insbesondere darum, die Befunde zu klassifizieren, mögliche Auswirkungen bei korrelierenden Schwachstellen auf die IT-Infrastruktur zu beurteilen und schließlich konkrete Handlungsempfehlungen zur Beseitigung aller gefundenen IT-Sicherheitslücken zu erarbeiten.

„Die technische Überprüfung hat gezeigt, dass wir hinsichtlich unserer IT-Sicherheit bisher gute Arbeit geleistet haben, da keine kritischen Mängel festgestellt wurden. Die ergänzenden Empfehlungen konnten wir, dank ausführlichem Bericht inklusive möglicher Lösungen, kurzerhand umsetzen. Den positiven Bericht nutzen wir darüber hinaus weiterhin auch als Nachweis in unserem ISO 27001-Audit“, fasst Florian Müller das White Box Audit zusammen.

„Unwissenheit schützt vor Hackern nicht“

Da nicht nur technische Schwachstellen Hackern die Möglichkeit geben, in Netzwerke einzudringen und Daten abzugreifen, wurde auch die Awareness der Mitarbeiter unter die Lupe genommen. Nach wie vor ist Phishing eines der beliebtesten Angriffsmittel. Unter einem fiktiven, aber sehr realistischen Vorwand täuschen Cyberkriminelle in präparierten E-Mails – die oftmals kaum von „echten“ Mails zu unterscheiden sind – den Empfänger, um so an seine Daten oder sein Geld zu gelangen. Nach der Überprüfung aller technischen Aspekte wurden daher auch gezielt Mitarbeiter der Stadtwerke Tuttlingen einem Awareness-Test unterzogen. Dazu informierten sich die Sicherheitsexperten zuerst über die bereits vorhandenen Verhaltensrichtlinien für die Mitarbeiter und legten anschließend gemeinsam mit den Verantwortlichen der Stadtwerke Tuttlingen die Rahmenbedingungen für die Testszenarios fest. Auf dieser Basis entwickelten die IT Security Experten das Layout und die Texte für diverse fingierte E-Mails.

Ohne das Wissen der Mitarbeiter wurden diese E-Mails in drei verschiedenen Kategorien verschickt. Sie konnten von den Empfängern leicht, mittel und schwer als Phishing-Mails identifiziert werden. Auf den Trick mit der offenen Zahlungsaufforderung der Bank fiel dabei kein Mitarbeiter herein. Anders sah es dann schon bei der gefälschten Mail eines Mitarbeiters aus, die die Kollegen über ihr neues Intranetportal informierte. Durch die persönlich gestaltete Ansprache und den

vertrauenswürdig wirkenden Absender wurde die Mail von 44 % der Empfänger geöffnet. Bis auf drei Personen klickten im nächsten Schritt alle auf den enthaltenen Link. 71 % der Personen, die den Link angeklickt haben, gaben zusätzlich ihre Zugangsdaten im Portal ein. Die Mail mit dem Schwierigkeitsgrad „hoch“ informierte die Mitarbeiter über ein kritisches Update auf dem Exchange-Server, das für Login-Probleme sorgte. Daher sollten nun auch die Empfänger ihren Login überprüfen. In diesem Szenario wurde die Mail von 9 der 19 Empfänger geöffnet, und 16 % gaben sogar ihre Zugangsdaten ein.

„Für uns war es sehr interessant zu sehen, mit welchen Tricks Hacker inzwischen ganz leicht an unsere Daten gelangen könnten. Unsere Mitarbeiter werden zwar regelmäßig geschult, aber bei einer Mail, die angeblich von einem Kollegen stammt, hörte das Misstrauen dann doch schnell auf“, sagt Florian Müller. Die Phishing-Kampagne diente gewissermaßen als Wake-up Call für die Mitarbeiter der Stadtwerke Tuttlingen. Sie gehen nun aufmerksamer und kritischer mit eingehenden E-Mails um und geben umgehend Warnungen oder Nachfragen an das IT-Team, sobald ihnen etwas seltsam erscheint.

FAZIT *Obwohl die Stadtwerke Tuttlingen bereits eine Vielzahl an IT-Sicherheitsmaßnahmen durchgeführt haben, entschieden sich die Verantwortlichen für eine externe Überprüfung durch Allgeier secion. Die umfassenden Sicherheitsüberprüfungen im Rahmen des White Box-Audits, in dem einzelne Systeme aus unterschiedlichen Hackerperspektiven analysiert wurden, lieferten eine Übersicht aller vorhandenen Schwachstellen. Das Ergebnis zeigte, dass sich der bisherige Einsatz der Stadtwerke Tuttlingen gelohnt hat und nur kleine Lücken bestanden, die schnell geschlossen werden konnten.*

Die zusätzlich durchgeführte Phishing-Kampagne mit fingierten E-Mails an die Mitarbeiter der Stadtwerke Tuttlingen machte zudem deutlich, dass Awareness und regelmäßige Schulungen für eine umfassende IT- und Informationssicherheit unbedingt erforderlich sind. „Die Zusammenarbeit mit Allgeier secion lief reibungslos ab, und wir haben sehr viel von den Experten gelernt. Aus diesem Grund sind wir aktuell in der Planung des nächsten gemeinsamen Projekts“, sagt Florian Müller.

© Copyright 2022

Urheberrechtshinweis
Alle Inhalte dieses Dokuments, insbesondere Texte, Fotografien und Grafiken, sind urheberrechtlich geschützt. Das Urheberrecht liegt, soweit nicht ausdrücklich anders gekennzeichnet, bei der Allgeier secion GmbH.

Stand: April 2022

Allgeier secion GmbH

Tel.: 040 38 90 71-0
Fax: 040 38 90 71-299
info@secion.de
www.secion.de

Paul-Dessau-Str. 8
22761 Hamburg