Cyber Security:

Herausforderungen bei Sensibilisierung und Projektmanagement

Cyber Security gewinnt zunehmend an Bedeutung. Pro Minute werden im Schnitt weltweit über hundert Angriffe verzeichnet und der dadurch verursachte Schaden soll laut einem Artikel des Cybercrime Magazine bis 2021 jährliche Kosten von 6 Billionen US-Dollar ausmachen.

Andreas Schneider

Gemäss dem Expertenbericht des Bundes zum Thema Cyberrisiken in der Schweiz ist das Spektrum von Übergriffen gross: Zerstörung von Webseiten, kriminelle Aktivitäten wie Phishing oder Erpressung mittels Denial-of-Service-Attacken, bis hin zu sehr gezielten Spionageangriffen und Sabotage an Infrastrukturen und Unternehmen. Viele Unternehmen investieren deshalb Tausende von Franken und Stunden von Arbeitszeit in Sicherheitslösungen, um sich vor diesen Übergriffen zu schützen.

Faktor Mensch als entscheidende Komponente

Doch auch mit den besten IT-Programmen für Cyber Security ist eine Organisation nicht vollumfänglich gegen Angriffe von aussen geschützt. Der Faktor Mensch bleibt die entscheidende Komponente, ob die IT eines Unternehmens geschützt bleibt oder Kriminelle Einlass finden. Diverse Studien zeigen, dass es zu über 80 Prozent menschliches Fehlverhalten ist, welches Kriminellen, vorbei an Sicherheitsmechanismen, Einlass in das unternehmerische Netz gibt. Entscheidend ist also, ob die Mitarbeitenden in ihren Unternehmen auf Cyberattacken und ihre Folgen geschult werden. Dass auf diesem Gebiet enormes Potenzial herrscht, haben bereits zahlreiche Unternehmen erkannt. Der globale Bildungsmarkt im Bereich Cyber Security wächst jährlich um 20 Prozent.

Geschulte Mitarbeitende minimieren Sicherheitsrisiken

Auch das Neuenburger Start-up Megaverse hat sich in diese Richtung spezialisiert und ist in den EdTech-Markt eingestiegen. Das Unternehmen hat eine Software entwickelt, mit derer die Mitarbeitenden auf spielerische Art und Weise den Umgang mit Cyber Security erlernen. Mithilfe von Artificial Intelligence (AI) geht Megaverse einen Schritt weiter als herkömmliche Plattformen. Durch spielerische Aufgabenstellungen passt sich das Programm automatisch dem Niveau des Benutzers an und zeigt den aktuellen Wissensstand in einer Übersicht und einem Report. Die Ersten, welche die Software von Megaverse in ihrem Unternehmen implementiert haben, sind unter anderem Helvetia, eine führende Privatbank sowie eine führende Uhrengruppe in Genf. «Diese erste Phase ist besonders attraktiv für die Kunden, da sie sich bei der Gestaltung und Umsetzung der Lernplattform aktiv einbringen können», sagt CEO Cécile Maye. Die Lernplattform ist rund um die Uhr zugänglich und als Desktoplösung, die 3D-Szenarien in real time (virtual, augmented und mixed) einsetzt, verfügbar. Das immersive Lernerlebnis stellt den Benutzern auf verschiedenen Niveaustufen insgesamt über 80 realitätsgetreue Aufgaben. Dies unter anderem in den Bereichen Internet, Hardware oder im Umgang mit Passwörtern. Die Mitarbeitenden werden so darauf sensibilisiert, welche Auswirkungen eine Cyberattacke auf sie selbst und das Unternehmen haben kann. Die adaptive Lernplattform kann unternehmensspezifisch angepasst werden, um möglichst realistische Szenarien zu kreieren. Megaverse ist Teil des EdTech Collider der EPFL in Lausanne. EdTech Collider ist die erste kollaborative Plattform in der Schweiz, die sich an Unternehmen richtet, die Bil-

Quelle: zVg

Experten im Security-Projektgeschäft: René Känzig (links) und Gianni Lepore (rechts) vom Berner Beratungsunternehmen Ironforge Consulting AG. René Känzig (à gauche) et Gianni Lepore de Ironforge Consulting à Berne sont des experts concernant la gestion de projet de la sécurité.

Andreas Schneider, F+W Communications, Bern. www.fwcom.ch

dung durch Technologie verändern wollen. Momentan hat die Plattform über 75 Mitglieder.

Das Projektmanagement als entscheidender Baustein im Cyber-Security-Umfeld

Cyber Security spielt auch im Behördenumfeld eine wichtige Rolle. Anfang dieses Jahres gab der Bundesrat den Startschuss für ein neu zu schaffendes Kompetenzzentrum im Bereich Cyber Security. Das Kompetenzzentrum soll eine nationale Anlaufstelle für Fragen zu Cyberrisiken werden. Der Bund muss jedoch nicht nur Bescheid wissen, sondern auch selbst gegen Cyberattacken geschützt sein. Ein Unternehmen, dass Security-Projekte im Bundesumfeld betreut, ist das ICT-Beratungsunternehmen Ironforge Consulting AG. Dass der Bund Unterstützung extern beantragt, sei keine Seltenheit, sagt Geschäftsführer Gianni Lepore. Denn ICT-Security-Anwendungen sind komplex und vielschichtig. Hinzu kommen die Ansprüche der verschiedenen Verwaltungseinheiten, die spezielle Prozesse haben, welche aufeinander abgestimmt werden müssen. Findet diese Abstimmung nicht statt, kann das dazu führen, dass die IT-Sicherheit beeinträchtigt ist. Gemäss Head of Sales, René Känzig, Ironforge AG, sind die Sicherheitsanforderungen für Projekte mit dem Bund anspruchsvoll. So werden sämtliche Projektmitarbeitende einer Personensicherheitsprüfung unterzogen und arbeiten anschliessend teilweise in geschützten, abhörsicheren Räumen. «Die Leistungsbezügerinnen und -bezüger der Bundesverwaltung wollen sich darauf verlassen, dass ausreichender ICT-Schutz vorhanden ist», so Känzig.

Überlegtes Vorgehen bringt gute Resultate

Oft wird mit dem Partner ein klar definierter Projektauftrag erarbeitet und ein zu lösendes Problem ist im Fokus, sagt Gianni Lepore. Die Bedürfnisse müssen zuerst herausgearbeitet werden, bevor mit dem eigentlichen Projekt begonnen werden kann. Bei ICT-Projekten im Bundesumfeld ist zudem ein klares Changemanagement von grosser Bedeutung. So wird vermieden, dass etwas umgesetzt wird, das nicht den geltenden Sicherheitsvorgaben entspricht. Gianni Lepore ergänzt: «Es ist von zentraler Bedeutung die Gegebenheiten in den verschiedenen Departementen richtig einzuschätzen, um die besten Lösungen zu finden, welche anschliessend auch im Betrieb effizient funktionieren.»

Es zeigt sich also, dass einerseits in der Projektierung, aber auch bei der anschliessenden Sensibilisierung der Mitarbeitenden auf spezialisierte Firmen zugegriffen werden sollte. Cyber Security ist ein delikates Thema, aber ein überlegtes Vorgehen bringt entsprechend gute Resultate.

Es ist also offensichtlich, dass einerseits bei der Projektierung, aber auch bei der anschliessenden Sensibilisierung der Mitarbeitenden ein gutes und umfassendes Projektmanagement von entscheidender Bedeutung ist. Alle betroffenen Bereiche, Abteilungen, Mitarbeitende und Unternehmensvorgaben, müssen mit einbezogen werden. Denn Cyber Security ist ein delikates Thema, welches präzises Vorgehen verlangt. ■

Cyber-sécurité:

Défis au niveau sensibilisation et gestion de projet

La cyber-sécurité devient toujours plus importante. D'après un article paru dans Cybercrime Magazine, plus d'une centaine d'attaques sont en moyenne enregistrées par minute dans le monde entier et les dommages causés devraient atteindre un coût annuel de 6 billions de dollars US d'ici 2021.

Andreas Schneider

Selon le rapport d'experts de la Confédération sur les cyber-risques en Suisse, le spectre des attaques est vaste : destruction de sites internet, activités criminelles telles que le phishing ou l'extorsion par des attaques Denial-of-Service, voire même des attaques d'espionnage très ciblées et le sabotage d'infrastructures et entreprises. Nombre d'entreelles investissent donc des milliers de francs et d'heures de travail dans des solutions de sécurité pour se protéger contre ces attaques.

L'essentiel du facteur humain

Mais même avec les meilleurs programmes informatiques pour la cyber-sécurité, une organisation n'est pas entièrement protégée contre les attaques extérieures. Le facteur humain reste l'élément essentiel pour déterminer si l'informatique d'une entreprise continue à être protégée ou si les criminels y ont accès. Diverses études montrent que l'erreur humaine est à l'origine du fait que plus de 80 pour cent de tous les criminels puissent accéder au réseau de l'entreprise en passant les mécanismes de sécurité. Le facteur décisif est donc de savoir si les employés sont formés par leur entreprise pour parer aux cyber-

Andreas Schneider PR F+W Communications, Berne. www.fwcom.ch

attaques et à leurs conséquences. De nombreuses entreprises ont déjà reconnu l'existence d'un énorme potentiel dans ce domaine. Le marché mondial de l'éducation en matière de cyber-sécurité connaît une croissance annuelle de 20 %.

Des employés formés pour minimiser les risques de sécurité

La start-up neuchâteloise Megaverse s'est également spécialisée dans ce domaine et est entrée sur le marché EdTech. L'entreprise a développé un logiciel qui permet aux employés d'apprendre à utiliser la cyber-sécurité de façon ludique. Avec l'aide de l'intelligence artificielle (IA), Megaverse va plus loin que les plateformes conventionnelles. Grâce à des tâches ludiques, le programme s'adapte automatiquement au niveau de l'utilisateur et affiche l'état actuel des connaissances dans un aperçu et un rapport. Helvetia, une première banque privée et un premier groupe horloger genevois ont été les premiers à implémenter le logiciel Megaverse dans leur entreprise. « Cette première phase est particu-lièrement attrayante pour les clients, car ils peuvent participer activement à la conception et à la mise en œuvre de la plateforme éducative », déclare Cécile Maye, CEO. La plateforme éducative est accessible 24 heures sur 24 et est disponible comme une solution de desktop utilisant des scénarios 3D en temps réel (virtuelle, augmentée et mixte). L'expérience éducative immersive offre aux utilisateurs plus de 80 tâches réalistes à différents niveaux, notamment dans les domaines d'internet, du hardware et de la gestion des mots de passe. Les employés sont ainsi sensibilisés à l'impact qu'une cyber-attaque peut avoir sur eux et sur l'entreprise. La plateforme éducative adaptative peut se conformer aux besoins spécifiques de l'entreprise afin de créer des scénarios aussi réalistes que possible. Megaverse fait partie du EdTech Collider de l'EPFL à Lausanne. EdTech Collider est la première plateforme collaborative en Suisse destinée aux entreprises qui veulent changer la formation par la technologie. La plateforme compte actuellement plus de 75 membres.

La gestion de projet en tant qu'élément clé de l'environnement de cyber-sécurité

La cyber-sécurité joue également un rôle important dans l'environnement fédéral. Le Conseil fédéral a donné son feu vert à la création d'un nouveau centre de compétences dans le domaine de la cyber-sécurité en début d'année. Le centre de compétences est appelé à devenir un point de contact national pour les questions relatives aux cyber-risques. Le gouvernement fédéral ne doit, cependant, pas seulement être conscient des cyber-risques, il doit aussi être lui-même protégé contre les cyber-attaques. L'entreprise de conseil en ICT Ironforge Consulting AG est une entreprise qui gère des projets de sécurité dans le contexte fédéral. Il n'est pas rare que le gouvernement fédéral sollicite une aide extérieure, déclare le directeur général Gianni Lepore. Les applications de sécurité ICT sont complexes et multidimensionnelles. Il y a aussi les exigences des différentes unités administratives avec des processus spéciaux qui doivent s'adapter les uns aux autres. Si cette coordination n'a pas lieu, la sécurité informatique peut être compromise. Selon René Känzig, directeur des ventes d'Ironforge AG, les exigences en matière de sécurité pour les projets avec la Confédération sont élevées. Tout collaborateur du projet est soumis à un contrôle de sécurité personnel et travaille ensuite dans des locaux protégés et à l'abri d'écoute. « Les destinataires des services de l'administration fédérale veulent s'assurer qu'il existe une protection suffisante en matière d'ICT », explique M. Känzig.

Une bonne gestion globale est important

Une mission de projet clairement définie est souvent élaborée avec le partenaire et l'accent est mis sur un problème à résoudre, déclare Gianni Lepore. Les besoins doivent être déterminés avant que le projet réel puisse être lancé. Une gestion du changement bien définie revêt également une grande importance pour les projets ICT dans le cadre fédéral. De cette façon, on évite de mettre en œuvre ce qui n'est pas conforme aux exigences de sécurité en vigueur. Gianni Lepore ajoute : « Il est primordial d'évaluer correctement les conditions dans les différents départements afin de trouver les meilleures solutions pour qu'elles soient ensuite parfaitement exploitables. »

Cela démontre que non seulement la planification des projets, mais aussi la sensibilisation des employés en résultant nécessitent l'intervention d'entreprises spécialisées. La cyber-sécurité est un sujet délicat, mais une approche mûrement réfléchie donne des résultats positifs.

Il apparaît donc évident qu'une bonne gestion globale du projet est d'une importance cruciale, que ce soit pour la planification du projet ou pour la sensibilisation ultérieure des employés. Tous les domaines concernés – départements, employés et directives de l'entreprise – doivent être inclus, car la cyber-sécurité est une question délicate qui nécessite une approche précise. ■