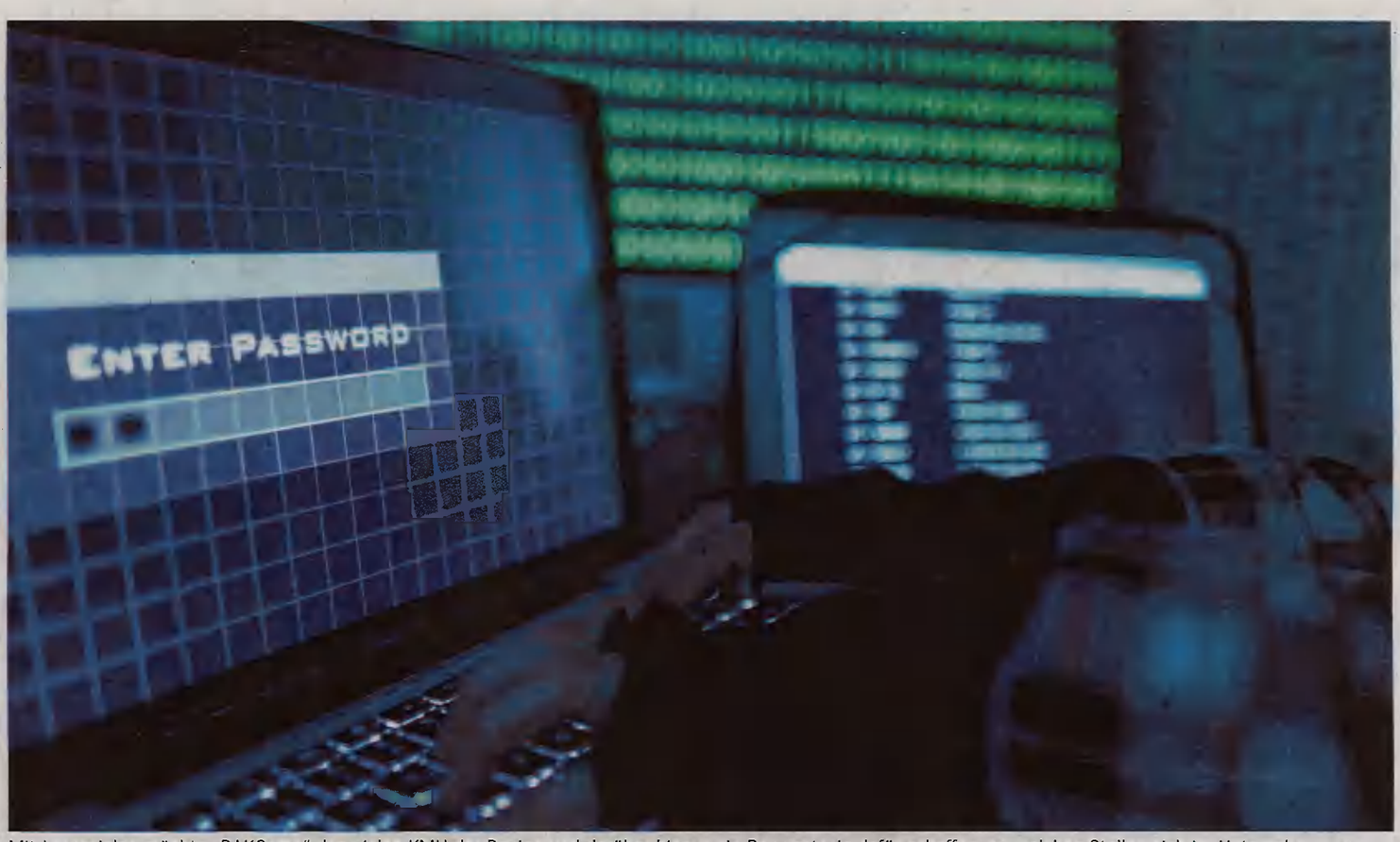

Mit Lernspielen möchte „BAKGame“ den vielen KMU der Region und darüber hinaus ein Bewusstsein dafür schaffen, an welchen Stellen sich im Unternehmen womöglich Sicherungslücken auftun könnten. FOTO: OLIVER BERG/DPA

Spielend sicherer werden

„BAKGame“ bringt KMU die Wichtigkeit von IT-Sicherheit mittels Gamification bei

Von Timo Lämmerhirt

AALEN – Kleine und mittlere Unternehmen (KMU) tragen in Deutschland in wesentlichem Maß zur gesamtwirtschaftlichen Leistung bei. Der Schutz dieser Zielgruppe vor Angriffen auf ihre IT-Sicherheitssysteme und die Absicherung der damit verbundenen Wirtschaftsleistung ist somit von höchster Bedeutung.

Seitens der KMU wird diese Bedrohung jedoch häufig unterschätzt. Hier tritt das Forschungsprojekt „BAKGame“ auf den Plan, das den KMU die notwendigen Fähigkeiten zur selbstständigen Risikobewertung zu vermitteln und über relevante Maßnahmen aufzuklären versucht, um die Absicherung der IT-Infrastruktur zu gewährleisten – und zwar spielerisch. Projektverantwortliche sind Prof. Dr. Marcus Gelderie von der Hochschule Aalen sowie Michael Nanz, Geschäftsführer der Technischen Akademie für berufliche Bildung Schwäbisch Gmünd.

Das WIRO, die Wirtschaftsförderungsgesellschaft für die Region Ostwürttemberg, hatte zu diesem Thema mittels eines virtuellen Vortrags geladen, in dem Hochschule und Technische Akademie „BAKGame“ vorgestellt haben. Gelderie ist seit 2018 Professor für IT-Sicherheit an der Hochschule Aalen mit dem Schwerpunkt Internet der Dinge. Schwäbisch Gmünd ist die Basis des kooperativen Studiengangs Internet der Dinge in Kooperation mit der Hochschule für Gestaltung, so ist die Verbindung der beiden Städte fast naheliegend.

„Das Thema IT-Sicherheit ist wichtig, ich weiß aber auch, dass es nicht einfach umzusetzen ist. Deswegen muss man dieses Thema auch mit einem gewissen Pragmatismus fahren“, sagt Gelderie. Das Projekt ist gestartet im November 2020 und läuft noch bis 2023. „BAKGame“ steht hierbei für Bedrohungsanalyse in KMU durch Gamification. „Wir haben die Vision, dass KMU eigenständig erkennen können, welchen Bedarf an IT-Sicherheit sie tatsächlich haben. Das heißt schlichtweg, dass man wissen muss, wo seine Baustellen sind. Das möchten wir mit diesem Projekt spielerisch näherbringen“, erklärt Gelderie, der es zugleich anhand eines Beispiels noch deutlicher machte: Man wisse, dass man ein Schloss an der Tür brauche,

> „Das führt schließlich zu einer Art Schockstarre: lieber gar nichts als etwas Falsches zu machen.“
>
> Prof. Dr. Marcus Gelderie, Hochschule Aalen

um sich zu schützen. Man wisse aber auch, dass man einen Schlosser für den Einbau benötige. „Man weiß also, was zu tun ist, kann es aber selbst nicht erledigen“, so Gelderie zur Ausgangsproblematik.

Hierfür ein Bewusstsein zu schaffen, Lösungsansätze zu finden, möchten die Projektpartner mithilfe ihrer entwickelten Lernspiele schaffen. „Wir möchten Gratisangebote entwickeln, die sich an die Arbeitsrealität der KMU richten, die versuchen, die Leute da abzuholen, wo sie sind und an dieses Thema heranzuführen. Gleichzeitig soll es sich mit den Alltagserfahrungen decken und nicht zu trocken akademisch sein“, fährt Gelderie fort. Am Ende dann soll das Sicherheitsniveau der KMU erhöht werden. Gleichzeitig sollen die Unternehmen derart sensibilisiert werden, dass dieses Niveau auch nachhaltig greifen kann. Die Zahl der Unternehmen, die durch Cyberangriffe finanziellen Schaden erlitten haben, ist in den vergangenen Jahren angestiegen, die Thematik somit aktuell. Problematisch sei häufig, dass speziell die KMU nicht über die stärksten finanziellen und personellen Ressourcen verfügten. Dabei werde heutzutage eine ganze Menge angeboten. Die Schwierigkeit entstehe dabei, zu entscheiden, was man speziell brauche für sein Unternehmen, was wirklich wichtig sein könnte. „Das führt schließlich zu einer Art Schockstarre: lieber gar nichts als etwas Falsches zu machen“, weiß Gelderie.

Dabei gebe es nicht die eine Bedrohung, die auf die einzelnen Unternehmen zukommen kann, nicht den einen Hacker, sondern zahlreiche. Es gebe eine ganze Reihe, die zum Teil auch gar nichts mit IT-Sicherheit zu tun haben. Dazu zählten auch Organisationen, die Malware (= Schadsoftware, d. Red.) ins Unternehmen einschleusen möchten oder das vom Baggerbiss zerstörte Glasfaserkabel. „Wir möchten diese Art von Kompetenz stärken durch Online-Lernspiele“, sagt Gelderie. In Form dieser Spiele zeigt das Team des Forschungsprojekts ebenfalls auf, was diese Bedrohungen konkret anrichten würden, um das Ganze zu visualisieren. „Wir vermitteln dabei einfach, dass die Risiken an ganz vielen Stellen in leicht anderem Gewand auftauchen.“ Es gehe dabei nicht darum, dass die Unternehmen künftig viel Geld in Sicherheitslösungen investieren, es gehe darum, ein Bewusstsein für die Probleme zu schaffen.

Um die Lernspiele entsprechend individuell an den Unternehmen auszurichten, analysiert die Forschungsgruppe gemeinsam mit den KMU den Sicherheitsbedarf. Anhand von Fragebögen werden die gesammelten Daten in Profile übermittelt, auf deren Basis Aus- und Weiterbildungskonzepte auf Basis von Gamification entwickelt werden. Die sämtlichen Lernspiele werden den KMU kostenlos zur Verfügung gestellt – so sollen die Unternehmen der Region am Ende spielerisch sicherer werden.

Das Projekt wird gefördert durch **„Mittelstand Digital“** (Das Projekt Bakgame ist Teil der Initiative **„IT-Sicherheit in der Wirtschaft“** im Förderschwerpunkt Mittelstand Digital), **„IT-Sicherheit in der Wirtschaft“** sowie dem Bundesministerium für Wirtschaft und Energie. **Weitere Informationen unter www.bakgame.de**, www.mittelstand-digital.de und www.it-sicherheit-in-der-wirtschaft.de, direkten Kontakt gibt es unter info@bakgame.de