

# IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Compliance



„Besser in Weiterbildung investieren, statt Lehrgeld zu bezahlen!“

*Interview mit Max Ziegler (Foto), Skytale Online Akademie und Olaf Beckmann, Audiocation*

## Cloud Security

- Hybride Umgebungen: Identity Management in der Cloud
- Cloud als Schutzpatron: Stolperfallen vermeiden
- Kontrolle: Cloud Access Security Brokers

## Identity/Access Management

- Abgespeckt: Komplexe IAM-Suiten sind out
- Digitale Transformation: Identität im Internet der Dinge
- Mobility: Smartphones ersetzen Schlüssel

## Markt, Technik und Test

- Datenschutz: Konsequenzen aus der neuen DS-GVO
- Sicherheitsstandards: Proaktive Strategien
- Im Test: Barracuda NextGen Firewall 6.1

Interview: Skytale zum Thema IT-Security Online-Seminare

## „In Weiterbildung investieren, statt Lehrgeld bezahlen!“

**Als unabhängiges Ausbildungsinstitut bietet Skytale Online-Kurse für IT- und Informationssicherheit. 2015 als Fachbereich bei Audiocation gegründet, lautet die oberste Prämisse, praktisch nutzbares Wissen in effektiver Weise zu vermitteln. Was zunächst wenig spektakulär klingt, hat innerhalb sehr kurzer Zeit einen bemerkenswerten Erfolgskurs eingeschlagen. Max Ziegler, Leiter der Skytale Online Akademie, und Olaf Beckmann, Gesellschafter-Geschäftsführer bei Audiocation, standen im Gespräch mit IT-SICHERHEIT Rede und Antwort zu Fragen nach Chancen, Grenzen und Praxis einer Online-Akademie im Hinblick auf ein so dynamisches und komplexes Thema wie IT-Sicherheit.**

**ITS:** IT-Sicherheit hat sich zu einer unglaublich komplexen Disziplin mit sehr vielen Facetten entwickelt. Wo setzen Sie mit Ihrer Online-Akademie an?

**Max Ziegler:** Komplex ist dieses Gebiet in der Tat. Selbst versierte Experten verlieren mittlerweile leicht den Anschluss und Durchblick, wenn sie die dynamischen Entwicklungen unterschätzen und nicht am Puls der Zeit bleiben – denn der ist rasend schnell.

Für den optimalen Lernerfolg setzen wir mit unserem Konzept deshalb auf der praktischen Ebene an: Erfahrene Spezialisten haben bei uns die Möglichkeit, ihr Know-how und ihre Fertigkeiten auf die Probe zu stellen. Dafür sorgen die Übungen und Aufgaben in unseren Onlinekursen, die einen starken Bezug zum Arbeitsalltag haben. Allen, die sich neu mit dem Thema IT-Sicherheit beschäftigen möchten, geben wir zusätzlich Orientierung an die Hand durch Tutorials, Fachinformationen und didaktisch optimierte Lektionen. Unser Ziel ist es, die Menschen zu befähigen, sich selbst einen Weg durch das Dickicht der Datensicherheit zu schlagen. Dazu liefern wir ihnen einen Kompass, die Werkzeuge und zeigen, wie sie funktionieren.

**Olaf Beckmann:** Der praktische Aspekt ist überaus wichtig. Daher setzen wir in den Kursen auf Übungen, die reale Gegebenheiten im Web eins zu eins nachbilden – wie bei einem Rätsel oder Puzzle. Daraus folgen zwei positive Effekte, die den herkömmlichen Konzepten wie Video-Tutorials oder Frontalunterricht völlig fehlen: Zum einen setzen sich die Kursteilnehmer selbst intensiv mit dem Stoff auseinander und betrachten mögliche Lösungswege aus verschie-

den Perspektiven. Zum anderen motivieren die Erfolgserlebnisse, die im Rahmen des interaktiven Ansatzes gesammelt werden. Deshalb ist der Lerneffekt wesentlich größer als bei einer trockenen Vorlesung, die schon vom Ansatz her wenig mit der Praxis zu tun hat.

**ITS:** Ein Kurskonzept für alle – egal auf welchem Niveau? Das scheint schwer vorstellbar. Wen adressieren Sie mit Ihren Kursen denn in erster Linie?

**Max Ziegler:** Ganz klar alle, die in das Thema IT-Sicherheit einsteigen oder dieses weiter vertiefen wollen und bereits einen soliden IT-Background haben. Sicherheit ist wie gesagt ein sehr fachübergreifendes Thema, das von der Netzwerktechnik bis hin zur Programmierung alle Bereiche berührt. Nach unserer Erfahrung ist es für IT-Spezialisten aus anderen Fachgebieten nicht leicht, während des täglichen Betriebs praxisbezogen in das Thema IT-Sicherheit einzusteigen. Schließlich haben sie auch eine große Verantwortung, ihre Projekte und Systeme zum Laufen zu bringen. Das Thema Sicherheit steht auch in der Ausbildung häufig an zweiter Stelle oder wird nur punktuell und nicht fachbezogen beleuchtet. Dazwischen sind die Aus- und Weiterbildungsangebote rar, die Brücken zwischen den Themen und Disziplinen schlagen.

**Olaf Beckmann:** Dennoch standen wir bei der Konzeption der Kurse vor der großen Herausforderung, jedem Kursteilnehmer etwas zu bieten. Denn zwangsläufig bringen sie individuelles Vorwissen, unterschiedliche Voraussetzungen und Kompetenzen mit. Wir haben die Kurse deshalb so gestaltet, dass die Teilnehmer alle notwendigen Hilfsmittel an die Hand bekommen, um die Aufgaben zu lösen. Stehen sie doch einmal vor einer unlösbaren Herausforderung, dann können wir im persönlichen Support den ein oder anderen entscheidenden Hinweis geben. Je größer das Vorwissen, desto mehr rücken dann die Aspekte Training, Routine und Wiederholung in den Vordergrund. Ganz nebenbei werden auch diese Kursteilnehmer über neue Methoden, Perspektiven und Ansätze stolpern, die ihn bei seiner täglichen Arbeit weiter voranbringen.

**ITS:** Haben Sie sich auf bestimmte Themenbereiche spezialisiert?

**Max Ziegler:** Davon sehen wir ab. Das Feld ist zwar weit, sodass es sinnvoll erscheint, die Kurse auf ausgewählte Aspekte zu fokussieren. Doch das birgt die Gefahr, dass wichtige Fachgebiete ausgeblendet werden. Wir haben uns deshalb dazu entschlossen, unseren

Studierenden nicht nur die Grundlagen zu vermitteln, sondern sie auch tiefer in verschiedene Themen zu führen. Selbstverständlich priorisieren wir dabei und decken mit unseren Kursen die wichtigsten Disziplinen ab: Angefangen bei der Sicherheit von Web-Applikationen und künftig auch Security Awareness, Netzwerksicherheit und Informationssicherheit. Unser Konzept ist jedoch offen für die Entwicklungen in der Branche und die drängenden Fragen, die daraus resultieren. Wir werden dann Antworten in der Weiterbildung finden und können flexibel darauf reagieren, was uns unsere Teilnehmer als Bedarf zurückmelden.

**ITS:** IT-Sicherheit braucht einen ganzheitlichen Ansatz, das wissen Sie als Security-Experten am allerbesten. Aber wie wollen Sie mit Ihren Einzelkursen diesem Anspruch gerecht werden?

**Olaf Beckmann:** Der ganzheitliche Ansatz fordert in erster Linie die Unternehmensführung und das Management heraus. In diesen Positionen benötigt das Personal den Blick für das große Ganze und Hintergrundwissen aus den verschiedensten Fachgebieten. Das konkrete, technische Know-how spielt hier zunächst eine untergeordnete Rolle. Auf der operativen Ebene sieht das anders aus. Die Entwickler, Programmierer und Administratoren sind bei der IT- und



Max Ziegler (links) und Olaf Beckmann kennen den Markt für Fort- und Weiterbildungen genau. Den zumeist einseitig auf Frontalunterricht ausgelegten Angeboten setzen sie ein interaktives, online-basiertes Lernkonzept entgegen.

Foto: Sara Moreira

Informationssicherheit mit spezifischen, technischen Fragen und Problemen konfrontiert. Dafür sind Fachwissen, Erfahrung und ein tieferes Verständnis der Zusammenhänge nötig. Unsere Kurse adressieren deshalb bewusst beide Gruppen, weil sie ja zusammen arbeiten müssen! Das gelingt viel besser, wenn man auch die Sichtweise des anderen versteht. Das ist nach unserer Erfahrung ein ganz zentraler Punkt. Viel zu häufig kommt es vor, dass die Mitarbeiter auf den unterschiedlichen Ebenen verschiedene Sprachen sprechen und deshalb aneinander vorbei reden. Das möchten wir verhindern und die Kommunikation zwischen allen Beteiligten verbessern.



Bei Skytale gibt es keine Anwesenheitspflicht. Tempo, Ort und Zeit definiert jeder Nutzer individuell – zum Beispiel auch mobil mit dem Smartphone in der Bahn.

**ITS:** Ein großes Problem haben in Deutschland besonders die Kleinunternehmen und Mittelständler. Ihre Daten sind für ihr Unternehmen genauso wertvoll und lebenswichtig wie das in Großunternehmen der Fall ist. Die Mittel zu ihrem Schutz – und dazu zählt ja auch die entsprechende Aus- und Weiterbildung der Mitarbeiter – sind aber meist arg begrenzt. Was raten Sie dieser Klientel?

**Max Ziegler:** Da sprechen Sie einen spannenden Punkt an, denn die KMUs stecken oft in einem Dilemma: Als Innovationstreiber sind sie in ihrer Branche ganz vorne mit dabei. Das macht sie für Hacker interessant, die innovative Ideen, Konzepte, vertrauliche und geheime Informationen stehlen wollen. Anders als bei den Großunternehmen und Konzernen können die Black-Hats davon ausgehen, dass gleich fünf Flaschenhalse für ein geringeres Schutzniveau bei den KMUs sorgen: Den Unternehmen fehlen häufig qualifiziertes Personal für IT- und Informationssicherheit, Zeit, Geld, technische Ressourcen und effektive Managementprozesse.

Dieses Dilemma ist real und jeder Unternehmer ist sich darüber absolut klar. Deshalb raten wir der Geschäftsführung und dem Management zu einer effektiven und zielführenden Strategie, die gemeinsam mit den Fachabteilungen ausgearbeitet werden muss. Die wichtigste Frage für den Start: Wo im Unternehmen liegen unsere Kronjuwelen im Sinne von Informationen und Prozessen? Erst wenn das geklärt ist, können die nächsten Schritte sinnvoll priorisiert und wirkungsvolle Schutzmaßnahmen entwickelt werden. Dazu braucht es dann natürlich qualifiziertes Personal, Zeit, Geld, technische Ressourcen und effektive Managementprozesse. Auch das muss jedem klar sein.

Ein weiterer Punkt: Proaktiv und präventiv handeln! Das geschieht in der Praxis häufig zu spät. Nämlich dann, wenn es schon zu einem kritischen Ereignis gekommen ist, das auch wirtschaftliche Schäden verursacht hat. Wir versuchen die Verantwortlichen dafür zu sensibilisieren, frühzeitig in das Know-how ihrer Mitarbeiter zu investieren anstatt Lehrgeld zu bezahlen. Denn die brauchen schließlich Zeit, um Sicherheitsmaßnahmen zu entwickeln und umzusetzen. Je früher man in der Entwicklung eines Systems oder einer Applikation das Thema Sicherheit integriert, umso günstiger und effektiver wird es am Ende.

**ITS:** Fort- und Weiterbildung sind durch die Diskussionen der vergangenen Monate vermehrt in den Blick der Unternehmen gerückt. Wie schätzen Sie die derzeitige Situation am Markt ein? Und wie unterscheiden sich Ihre Kurse von den Angeboten anderer Anbieter?

**Olaf Beckmann:** Nach unserer Einschätzung ist das derzeitige Angebot sehr einseitig ausgerichtet. Im Netz wimmelt es von Fachbeiträgen, Büchern, Video-Tutorials und Fernkursen, die – teils noch auf Papier per Post verschickt – darauf fokussieren, Lernstoff in Multiple-Choice-Bögen abzufragen. Diese Art der Fortbildung ist nicht nur mühsam. Für die wenigsten Menschen ist dieser „Frontalunterricht“ überhaupt geeignet, komplexe Zusammenhänge zu verstehen, das Wissen anzuwenden und auf andere Sachverhalte zu übertragen. Was bietet diese Methode? Input! Was fehlt Ihr? Output! Denn für den optimalen Lernerfolg muss das Gehirn nicht nur Informationen aufnehmen, sondern auch verarbeiten, kombinieren, in anderer Form wieder ausgeben.

Wir erreichen das durch die Konzeption der Übungen und Aufgaben. Für unseren Online-Kurs „Sicherheit von Web-Applikationen“ zum Beispiel haben wir eine virtuelle Maschine aufgesetzt, die einen kompletten Online-Shop für Kaffeespezialitäten abbildet – mit Ka-

talog, Warenkorb, Kasse, Kundendatenbank, allem Drum und Dran. Diesen haben wir gespickt mit typischen Sicherheitslücken, die es im gesamten Kursverlauf zu finden gilt. Wie bei einem kniffligen Sudoku wird das Gehirn die ganze Zeit auf Trab gehalten. Denn möglicherweise zeigt der Lernstoff mehrere Lösungswege auf. Oder ein unbedeutendes Detail zu Beginn des Kurses liefert im weiteren Verlauf die entscheidende Information, um eine komplexe Sicherheitsbarriere zu knacken. Unsere Methode ist nicht nur didaktisch sinnvoll, sie orientiert sich auch nah an den täglichen Herausforderungen bei der Arbeit. Ganz nebenbei macht diese Herangehensweise auch noch eine Menge Spaß und wir alle wissen: Mit Spaß lernt es sich am besten. Hat man erst einmal verstanden, wie der Angriff funktioniert, erschließt sich der Schritt zur Verteidigung, also zur Behebung der Schwachstelle, in der Regel sehr schnell.

**ITS:** Ich verstehe. Doch wie läuft der Unterricht konkret ab? Wie melde ich mich an und wie geht es dann weiter? Schildern Sie doch bitte kurz die organisatorischen Abläufe, die hinter Ihrem Konzept stehen.

**Max Ziegler:** Nach der Anmeldung auf unserer Website erhalten die Teilnehmer einen eigenen Nutzer-Account für den gebuchten Kurs, der via Browser aufgerufen wird. Dort sind alle Informationen, Werkzeuge und Aufgaben hinterlegt und die Studierenden können intuitiv durch die Kursmodule navigieren. Hier erhält auch jeder seine eigene virtuelle Maschine, die ihm im Verlauf des Kurses als „Lernobjekt“ beziehungsweise Angriffsziel dient. So etwas wie Anwesenheitspflicht gibt es dabei selbstverständlich nicht. Ort und Zeit definiert jeder Nutzer individuell – am Arbeitsplatz, in der Bahn oder daheim nach Feierabend. Tempo und Intensität kann man also selbst bestimmen.

Lediglich den Ablauf und die Abfolge der Lektionen und Aufgaben haben wir weitestgehend festgelegt und darauf geachtet, dass der zeitliche Aufwand optimal auf berufstätige Personen abgestimmt ist. Beispielsweise bevorzugen Selbstständige meist kleinere Einheiten nach Feierabend, so dass es möglich ist, den Kurs über mehrere Wochen laufen zu lassen. Doch es spricht nichts dagegen, das Tempo zu erhöhen, wenn es der Arbeitsalltag oder die berufliche Situation zulassen. Oder eben zu pausieren, wenn es beruflich oder privat doch mal eng werden sollte.

**ITS:** Führen Sie im Verlauf der Kurse Tests durch? Falls ja, wie läuft das ab?

**Olaf Beckmann:** Selbstverständlich messen wir während der Kurse die Leistungen unserer Studierenden – allerdings nicht in Form von expliziten Fragebögen zu einem bestimmten Zeitpunkt, wie man es vielleicht von den Klausurphasen an der Uni kennt. Vielmehr dokumentiert unser System kontinuierlich die individuellen Fortschritte und Ergebnisse der gelösten Aufgaben anhand eines Punktesystems. Einerseits dient das der Selbstkontrolle der Studierenden. Andererseits werten wir die Informationen am Ende des Kurses aus, um die Leistungen abschließend und individuell zu beurteilen.

**ITS:** Gibt es dann eine Art Zeugnis oder Zertifikat? Falls ja, welchen Wert hat das auf dem Markt? Gibt es irgendwelche offiziellen Anerkennungen?

**Max Ziegler:** Vorausgesetzt, der Kurs wird mit der erforderlichen Mindestpunktzahl abgeschlossen, erhalten die Studierenden ein Skytale-Zertifikat. Wir garantieren eine hohe Qualität unserer Fortbildungskurse durch ein zertifiziertes Qualitätsmanagementsystem nach ISO 9001, eine Zulassung der staatlichen Zentralstelle für Fern-

**03 - Schwachstellen in Webapplikationen**

- 1 Grundziele für dieses Kursmodul
- 2 Grundlagen SQL Injection
- 3 Blind SQL Injection
  - Blind SQL Injection
  - Daten mit Blind SQL Injection abfragen
  - Sonderfall - Time based Blind SQL Injection
  - Grid- und Kiernachreibung
- 4 Error Based SQL Injection
- 5 Firewall Evasion / Encoding
- 6 Erweiterte Anwendungsfälle
- 7 Speicherung von Passwörtern
- 8 Automatisierte Angriffe auf Datenbanken

**BEISPIEL**

Die Applikation wird also mittels `SELECT` den Statuscode aus der Datenbank abfragen und dann in einen lesbaren String übersetzen, in etwa folgendermaßen (als vereinfachter Pseudocode dargestellt):

```

$result = database_query ( "SELECT availability FROM stock WHERE article_id = " + $userinput )
switch ($result) {
  case -1:
    $printable_result = "nicht mehr lieferbar"
  case 0:
    $printable_result = "Status unbekannt"
  case 1:
    $printable_result = "lieferbar"
  [... weitere Cases gefälligst ...]
}
echo „Der von Ihnen angefragte Artikel ist “ + $printable_result

```

Sie sehen, dass die Ausgabe aus der Datenbank in diesem Fall **nicht direkt von der Applikation angezeigt** wird. Hier liegt aber trotzdem eine SQL Injection Schwachstelle vor (erkennbar an der ungefilterten Verwendung des `UserInput`), die wir ausnutzen können.

Auch wenn Blind SQL Injection auf den ersten Blick **schwieriger auszunutzen** und weniger effektiv zu sein scheint - die Auswirkungen sind am Ende **die gleichen** wie bei der „normalen“ SQL Injection. Das Auslesen von Daten ist eben (manuell) nur deutlich aufwändiger.

**WISSEN**

Das Vorgehen ist dabei relativ simpel:

Nachdem man sich sicher ist, dass wirklich eine Blind SQL Injection Schwachstelle vorliegt und ein gültiges Statement zusammen setzen kann (s.o.), ist man schon kurz vor dem Ziel. Oben wurde schon der Begriff „Tautologie“ beschrieben (immer wahre Klausel wie `1=1`). Jetzt brauchen wir sie wieder.

Im Skytale-Kurs „Sicherheit von Web-Applikationen“ dient den Studierenden eine virtuelle Maschine als Angriffsziel. Diese bildet einen kompletten Online-Shop für Kaffeespezialitäten ab und ist gespickt mit typischen Sicherheitslücken, die es im Kursverlauf zu finden gilt.

unterricht (ZFU) nach Fernunterrichtsschutzgesetz (FernUSG) und ein Zertifikat nach der Akkreditierungs- und Zulassungsverordnung Arbeitsförderung (AZAV). Die ZFÜ überwacht die Angebote am Markt, prüft die Seriosität und stellt hohe Anforderungen an die Inhalte und didaktischen Konzepte.

Doch letztlich entscheidet der Erfolg unserer Teilnehmer in ihren Unternehmen über den Marktwert der Zertifikate. Klar wertet ein erfolgreich absolvierter Kurs den Lebenslauf auf. Aber ob es Einstellungskriterium für die offene Stelle wird, hängt davon ab, ob der Einzelne damit die Voraussetzung schafft, ein Unternehmen erfolgreich gegen aktuelle Bedrohungen zu schützen. Dafür ist es wichtig, dass er sein neu erworbenes Wissen ins Unternehmen trägt und aktuell hält. Die beste Basis dafür sind unsere hochkarätigen Dozenten, die aus der Industrie kommen und dort jahrelang international relevante Unternehmen geschützt haben.

**ITS:** Anbieter von Cloud-Security-Lösungen haben Konjunktur. Die Verheißung: Wir kümmern uns um eure Sicherheit – ihr kümmert euch um euer Geschäft. Was halten Sie von diesem Ansatz? Ist die Weiterbildung der eigenen Mitarbeiter damit hinfällig?

**Max Ziegler:** Es wäre grob fahrlässig, die gesamte Verantwortung für die Informationssicherheit ebenfalls in die Cloud beziehungsweise in die Hände des Anbieters zu legen. Awareness und Client-Security wären zum Beispiel Stichworte. Denn auch wenn die Daten und Informationen in einem Rechenzentrum höchster Schutzklasse liegen, sind es nach wie vor die Mitarbeiterinnen und Mitarbeiter, die durch Berechtigungen und Zugriffsrechte täglich mit den Daten arbeiten. Das bedeutet auch, dass sie prinzipiell Schaden anrichten können. Auch die beste Cloud-Lösung schützt nicht vor Social Engineering oder Ransomware. Denn die Black-Hats suchen nach

dem einfachsten Weg, ihre böartige Software unters Volk zu bringen. Und der führt meist über den Desktop eines unvorsichtigen Mitarbeiters. Ein gewisses Grundverständnis in puncto IT-Sicherheit ist also bei jedem Mitarbeiter notwendig.

Darüber hinaus bietet die Cloud-Lösung oft nicht alle benötigten Anwendungen. Werden beispielsweise maßgeschneiderte oder selbst entwickelte (Web-)Applikationen gebraucht, sollte man bei der Konzeption, Entwicklung und kontinuierlichen Überprüfung nach Updates auch die Stolperfallen kennen und umgehen können. Dabei ist es egal, ob die Applikation nun in der Cloud oder im eigenen Rechenzentrum betrieben wird.

**Olaf Beckmann:** Einen weiteren, wichtigen Punkt möchte ich gern ergänzen: Wer beurteilt, ob der Cloud-Service wirklich sicher ist? Wie Sie schon mit Ihrer Frage richtig andeuten, ist das oftmals mehr eine Verheißung denn ein Versprechen oder gar Wirklichkeit. Im Unternehmen brauche ich also Mitarbeiter, die das Angebot des Cloud-Dienstes auf Herz und Nieren prüfen und anschließend bewerten können. Sind auch die Schnittstellen zur Cloud und die Anbindung an die eigene Infrastruktur sicher? Wie steht es um die Ausfallsicherheit und Verfügbarkeit? Das sind wichtige Fragen und niemand sollte erwarten, dass die belastbaren Antworten von dem Anbieter kommen.

**ITS:** Wenn es um Netzwerksicherheit geht, hängt ja vieles mit den eingesetzten Switches und Routern zusammen. Arbeiten Sie hier mit bestimmten Herstellern der IT-Sicherheits-Branche zusammen? Wie herstellerabhängig sind Ihre Kurse?

**Olaf Beckmann:** Wir vermitteln in unseren Kursen technische Grundlagen, allgemein gültige Prinzipien und systematische Zusammenhänge, die unabhängig vom Hersteller immer und überall gel-

## Die Interviewpartner:

**Max Ziegler** hat Diplom-Informatik an der Universität Paderborn und am RMIT Melbourne studiert. Anschließend war er fünf Jahre bei einem renommierten IT-Sicherheitsunternehmen als Berater im Bereich IT- und Informationssicherheit tätig. Neben Sicherheitsüberprüfungen für große Unternehmen im europäischen Raum hat er Trainings zur Sicherheit von Web-Applikationen, Betriebssystemen und Netzwerken durchgeführt und an verschiedenen Hochschulen unterrichtet. In mehreren Jahren als IT Security Officer, Head of IT-Infrastructure und Leiter der Informationssicherheit beim Automobilzulieferer Hella baute er dort den Bereich IT- und Informationssicherheit weiter aus. Max Ziegler entwickelt und leitet die Skytale Online Akademie für IT-Sicherheit bei der Audiocation GmbH, die seit 2009 webbasierte Fort- und Weiterbildungen anbietet.



**Olaf Beckmann** begann seine IT-Laufbahn in der Abteilung Datenbank Architektur und Softwareentwicklung des Fraunhofer Instituts für Informationsverarbeitung in Technik und Biologie (IITB) in Karlsruhe. Nach mehreren Jahren dort hat er anschließend Diplom-Informationstechnik an der dualen Hochschule Stuttgart studiert und im Rahmen des dualen Studiums mehrere Jahre bei der becos GmbH im Bereich Softwarearchitektur und Entwicklung gearbeitet. Nach Abschluss seines Studiums war er parallel als freier Dozent für die europäische Fernhochschule Hamburg tätig. Seit 2009 ist Olaf Beckmann Gesellschafter-Geschäftsführer der Audiocation GmbH und unter anderem verantwortlich für die Qualitätssicherung der Online-Kurse.



ten. Wir möchten unsere Studierenden befähigen, dieses Wissen dann selbst auf den konkreten Einzelfall anzuwenden oder die Produkte der Branche hinsichtlich Anforderung und Eignung selbst zu bewerten.

**ITS:** Wie reagieren Sie auf aktuelle Trends? Beispielsweise hat sich die IT-Sicherheitsindustrie gerade bis auf die Knochen blamiert, weil sie bei einem so fatalen Thema wie erpresserischer Datenverhaftung – die sowohl von Firmen wie auch Privatpersonen so gefürchtete Ransomware – viel zu lange ziemlich nackt da stand. Mehr als ein bisschen Besserwisserie und ein wenig eigene Produkte unterjubeln wollen kam da nicht. Fließt sowas in Ihre Kursplanung mit ein?

**Max Ziegler:** Ja, selbstverständlich greifen wir auch aktuelle Entwicklungen auf. Der dringende Handlungsbedarf leitet sich ja nicht nur aus Ihrem Beispiel ab, sondern aus den vielen Schwachstellen, die die Branche derzeit beschäftigen. Doch gleichzeitig dürfen die teils dramatischen Ereignisse nicht über die tieferliegenden Ursachen hinwegtäuschen. Schließlich sind es auch im Fall der Ransomware die Menschen, die der schädlichen Software Tür und Tor zu den Systemen öffnen – meist aus Unkenntnis oder Unachtsamkeit. Ich habe in meiner Arbeit als Sicherheitsexperte die Erfahrung gemacht, dass sich die Geschichte in diesem Punkt zu wiederholen scheint: Die Fehler bleiben stets die gleichen. Was sich ändert sind die Technologien, die von einer stets neuen Generation entwickelt und genutzt werden.

Nehmen Sie zum Beispiel die sichere Verschlüsselung im Online-Banking. Eigentlich ein alter Hut. Die wichtigsten Fragen hierzu hat die Branche vor mehr als zwanzig Jahren schon beantwortet. Doch heute wird die Technologie von einer neuen Generation auf die Smartphones, Tablets und Apps übertragen – und es ist erschreckend festzustellen, wie oft in den Anfängen der Smartphone-Apps

die saubere Prüfung von SSL-Zertifikaten fehlte! Das gleicht einem Déjà-vu, weshalb wir unsere Aufgabe in der Fort- und Weiterbildung vor allem darin sehen, ein solides Fundament und Verständnis für Grundlagen und Konzepte zu legen. Nur dann werden die Menschen und Unternehmen in die Lage versetzt, effektive Abwehrmaßnahmen gegen jede Art von Schadsoftware zu entwickeln.

**ITS:** Wo sehen Sie für dieses Jahr die größten Gefahren für die IT-Sicherheit und wo wollen Sie dementsprechend künftig weitere Schwerpunkte setzen?

**Olaf Beckmann:** Die größte Gefahr liegt vielleicht darin, dass zu viel über das Thema IT-Sicherheit geredet und zu wenig getan wird (lacht). Aber mal Spaß bei Seite. Mit großer Sorge betrachten wir die neuen Strategien der Black-Hats, die immer weniger Energien darauf verschwenden, direkt die komplexen und bestens gesicherten High-Tech-Systeme zu knacken. Denn – auch das möchte ich betonen – viele Entwickler und Administratoren haben ihre Systeme und Netzwerke sehr gut im Griff. Stattdessen gehen die Hacker nun verstärkt Umwege, die jedoch bequemer zum Ziel führen. Sie nehmen die Anwender, Nutzer und Clients ins Visier – und damit das schwächste Glied der Kette. Diese Entwicklung betrifft also alle, die IT-Systeme nutzen, und nicht nur den engen Kreis der IT-Spezialisten. Mit Sicherheit wird daher das Thema Security Awareness unser nächster Schwerpunkt werden.

**ITS:** Vielen Dank für das Gespräch!

Das Interview führte Stefan Mutschler, stellvertretender Chefredakteur IT-SICHERHEIT

## Über Skytale

Die Skytale Online Akademie für IT-Sicherheit ist eine Marke der Audiocation GmbH. Die Kurse sind zugelassen von der Staatlichen Zentralstelle für Fernunterricht (ZFU) nach Fernunterrichtsschutzgesetz (FernUSG). Kursteilnehmer können damit von Fördermaßnahmen öffentlicher Träger profitieren. Der Name Skytale (griechisch: „scytale“; ‚Stock‘, ‚Stab‘) ist dem ältesten bekannten Kryptographieverfahren entlehnt. Es wurde bereits vor mehr als 2500 Jahren in Sparta genutzt, um Botschaften zu verschlüsseln.



**SKYTALE**®  
ONLINE ACADEMY FOR IT SECURITY