Sylvia Johnigk

Warum Hacken überzeugt und IT-Sicherheit langweilt

Neulich, in der Kantine bei einem Auftraggeber, sprachen wir über das Image von Hackern und IT-Sicherheitsspezialisten. IT-Sicherheitsspezialisten, vor allem Interne, also Angestellte, genießen in Unternehmen das Image des Spielverderbers. Das Management möchte neue innovative Produkte einsetzen und jedes Mal steht da ein IT-Sicherheitsspezialist, der seine Bedenken, also Sicherheitslücken, aufzeigt, die dazu führen, dass Unternehmensdaten oder gar Kundendaten abhandenkommen können. Für das Management ein Ärgernis, die Welt ist voller Möglichkeiten, die *„ganze Welt"* darf sie einsetzen und vor ihnen steht ein Bedenkenträger, der dies verhindern und ihnen das *Spielzeug* wegnehmen möchte.

Für das Management sind solche Unzulänglichkeiten lästig, sie wollen das Produkt trotzdem. Sie fordern vom IT-Sicherheitsspezialisten eine Lösung, die es ermöglicht, das Produkt möglichst in seiner ganzen Vielfalt nutzen zu können. Natürlich dürfen Sicherheitsmaßnahmen nur wenig kosten, es sei denn, die IT-Sicherheitsspezialisten erbringen den Beweis, dass ihre Befürchtungen nicht nur ihrer wild gewordenen Fantasie entspringen.

Der einzige Weg, dem Management Zustimmung und Budget abzuringen, ist, einen *externen* Hacker zu kennen, der nicht nur Hacken kann, sondern auch einen Anzug besitzt, ihn trägt und in einer Management-kompatiblen Sprache einen *Live Hack* zeigen kann. Das macht Eindruck. Zumindest für einen kurzen Augenblick, den die IT-Sicherheitsspezialisten schnell nutzen müssen, um ein Budget zu bekommen. Damit die Sicherheitsmaßnahmen umgesetzt werden können, die sie vorgeschlagen haben. Fazit: Sie bekommen ihr Budget, aber warum?

Live Hacken ist unmittelbar, man kann es *„fast anfassen"*. Zumindest kann man *es* mit eigenen Augen sehen. Das System ist gehackt, die Daten wurden entwendet. Der Beweis wurde erbracht. Wenn der *Live Hack* dann noch ein Spektakel ist, so hinterlässt das manchmal sogar einen bleibenden Eindruck.

Ganz anders ist es mit der IT-Sicherheit. Sie zu zeigen ist unspektakulär. Wenn IT-Sicherheitsspezialisten einen richtig guten Job gemacht haben, passiert nichts, was einer Erwähnung wert wäre. Das ist wie ein Krimi ohne Tote, ein Formel-Eins-Rennen ohne Unfall oder ein Fußballspiel ohne Foul und Tor. Das ist nicht nur langweilig, sondern richtig langweilig – leider. Machen wir einen Selbstversuch. Stehen Sie auf, gehen Sie vor einen Spiegel und stellen Sie sich vor, Sie stehen vor Ihren Managern. Und dann sagen Sie dynamisch und kraftvoll: *„Es ist nichts passiert! Ich möchte ein Budget, damit weiterhin nichts passiert."* Und? Haben Sie sich selbst überzeugt? Würden Sie sich ein Budget geben, damit nichts passiert? *„Nichts passiert"*, das ist wie Stillstand und ärgerlich für den IT-Sicherheitsspezialisten, der sich letztendlich dieselben Gedanken macht wie der Hacker, nur dass der IT-Sicherheitsspezialist die Sicherheitslücken voraussieht und gleich die notwendigen Sicherheitsmaßnahmen umgesetzt hätte, wenn das Budget da gewesen wäre. So muss er warten, bis das Produkt fertiggestellt ist und ein Hacker mittels eines Penetrationstests die Sicherheitslücken aufzeigt, die man schon vorher gesehen hat. Bei IT-Sicherheitsspezialisten kommt da ein wenig Frust auf.

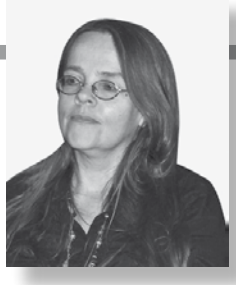
Hacken ist Aktivität. Der Hacker wirkt kraftvoll, dynamisch, belebend. Er ist ein Macher, der energiegeladen die Tür eintritt, wenn sie ihm nicht geöffnet wird. Er redet nicht nur davon, dass IT-Systeme verwundbar sind, er führt es den Zweiflern vor. Er zeigt damit den Stinkefinger. Und obwohl das Management darüber verärgert sein müsste, ist es begeistert. Endlich jemand, der mit der Faust auf den Tisch schlägt, sich durchsetzt und nicht nur so daher redet.

Das Problem ist, Hacker sind nötig, um das Management zu überzeugen, weil Taten offensichtlich besser wirken als Worte. Dabei darf man aber nicht vergessen, dass es wesentlich einfacher ist, ein existierendes System auseinander zu nehmen und es zu hacken, als ein neues IT-System zu entwickeln, das frei von Sicherheitslücken ist. Die Ungleichheit besteht darin, dass der Hacker nur eine einzige Sicherheitslücke finden muss, während der IT-Sicherheitsspezialist alle Sicherheitslücken finden und schließen muss, bevor das IT-Produkt ausgeliefert wird.

Das Beste wäre, wenn Hacker und IT-Sicherheitsspezialisten enger mit den Entwicklern zusammenarbeiten würden. Vor allem müssten beide in die gesamte Produktentwicklung integriert werden, um gemeinsam die Sicherheitslücken frühzeitig zu entdecken und zu schließen. Dazu müssten Hacker nicht nur *„destruktiv sein und kaputtmachen"*, sondern ihr Können nutzen, um Sicherheitslücken von vornherein zu vermeiden. Möglicherweise beißt sich da die Katze in den Schwanz, teure Sicherheitsmaßnahmen lassen sich nur rechtfertigen, wenn der Beweis erbracht wird, dass ein Sicherheitsproblem tatsächlich existiert und nicht nur ein Hirngespinst ist. Die Existenz eines Sicherheitsproblems lässt sich nur beweisen, wenn das System existiert und man es live hackt.

Im Übrigen, wenn ein IT-System mal nicht gehackt werden kann, so hat der IT-Sicherheitsspezialist noch lange keinen guten Job gemacht. Viel wahrscheinlicher ist, dass der Hacker seinen Job nicht gut genug gemacht hat. Oder?

Sylvia Johnigk



Sylvia Johnigk studierte Informatik an der TU Berlin und befasste sich schon im Studium mit Themen wie Datenschutz und Informationssicherheit. Sie arbeitete fünf Jahre in der Forschung und acht Jahre bei einem Finanzdienstleister. Seit 2009 ist sie selbständig und leitet ein kleines Unternehmen in München, das sich auf Beratung von Unternehmen zum Thema Informationssicherheitsmanagement mit dem Schwerpunkt Mitarbeitersensibilisierung spezialisiert hat.