

# Handeln statt Wissen

Aktueller Phishing-Benchmark beweist: Mit Security Awareness alleine ist es nicht getan. Knapp 20 Prozent der Portalbesucher hinterliessen persönliche Angaben.



Quelle: Cassarius

**Security Awareness** – kaum ein Sicherheitsbeauftragter der nicht davon spricht. Unter der Annahme, dass aus Wissen das richtige Handeln folgt, wird dabei oftmals nur auf Informationsvermittlung gesetzt. Die tägliche Erfahrung zeigt jedoch, dass aus theoretischem Wissen noch lange kein entsprechendes Handeln hervorgeht.

Die aktuelle Studie von CASSARIUS Confidence bestätigt diese Aussage. Das auf Informationssicherheit spezialisierte Beratungsunternehmen, führte im Frühjahr 2011 zum zweiten Mal eine vergleichende Analyse (Benchmark) zu Mitarbeiterverhalten im Umgang mit E-Mail durch. Ein von CASSARIUS präpariertes Phishing Mail wurde ohne Vorwarnung an die insgesamt 12871 Mitarbeitenden der 28 teilnehmenden Organisationen versandt.

Mit dem Versprechen schöner Gewinne und spannender Rabatte lockte CASSARIUS die Teilnehmenden auf eine eigens präparierte Webseite, ein angeblich neues Ticketportal für die Schweiz und forderte die Interessenten auf ein Benutzerkonto einzurichten.

Die Sicherheitsberater von CASSARIUS werteten anschliessend pro teilnehmender Firma aus, wie viele Mitarbeitende auf einen der Hyperlinks im Phishing-Mail klickten und wie viele auf der präparierten Webseite persönliche Angaben hinterliessen. Das Ergebnis: 599 Personen (4,65%) benutzten die Links im E-Mail und wurden auf das vorgetauschte Portal weitergeleitet. 117 Portalbesucher haben zudem ein Benutzerkonto inklusive Passwort eingerichtet sowie weitere persönliche Angaben hinterlassen. Das entspricht 19.5 Prozent.

Diese Ergebnisse zeigen einmal mehr: Selbst wenn Mitarbeitende die theoretischen Risiken kennen, verhalten sie sich im Geschäftsalltag oft unglücklich – «Eine Tatsache, die wir immer wieder antreffen,» sagt Marcel Oberli, Leiter CASSARIUS Confidence, «weil Mitarbeitende das richtige Verhalten weder geübt noch automatisiert haben».

## Security Behaviour

CASSARIUS Confidence beschäftigt sich seit Jahren mit dem Thema Mitarbeitersensibilisierung für Informationssicherheit und führt diverse Schulungen und Kampagnen bei unterschiedlichsten Kunden durch. Was dabei auffällt: Die Security Awareness der Mitarbeitenden ist sehr gut! Dank klar kommunizierten Sicherheitsrichtlinien, regelmässiger Berichterstattung über neue Attacken und Risiken sowie der zunehmenden Computer-Affinität der Mitarbeitenden selbst, sind sich die meisten der lauenden Gefahren auf Computern durchaus bewusst.

«Das Ziel von Sicherheitsbeauftragten muss es sein, dass sich Mitarbeitende richtig verhalten und nicht nur, dass sie wissen wie sie sich verhalten sollten,» so Oberli. Ein kleiner aber entscheidender Unterschied. Security Behaviour lautet denn auch das Motto der Kampagnen von CASSARIUS. Die Mitarbeitenden sollen mit den Gefahren konfrontiert werden und durch das Erlebnis lernen, wie man sich richtig verhält. Marcel Oberli: «Unsere Kunden erhalten nach jeder Aktion – d.h. nach jeder Konfrontation mit einem typischen Sicherheitsrisiko, eine verlässliche Aussage, wie viele Mitarbeitende sich bei versuchten Angriffen per E-Mail, im Internet, oder mit mobilen Datenträgern korrekt verhalten. Die Mitarbeitenden ihrerseits lernen die Gefahren hautnah kennen und können das richtige Verhalten entsprechend erlernen. Dabei ist einmal erleben bekanntlich besser als zehnmahl hören.»

## CASSARIUS

[www.cassarius.ch/confidence](http://www.cassarius.ch/confidence)  
[confidence@cassarius.ch](mailto:confidence@cassarius.ch)

26.05.2011: Security Breakfast, Den Hackern auf den Fersen Anmeldung erforderlich