IT in der Praxis:
Wie man in Unternehmen eine Kultur der Cybersicherheit schafft

Nicht wichtig weil „es eh nur die Großen" trifft, weil „man immer erst hinterher schlauer ist" und schon gar nicht weil es „nicht meine Baustelle" ist? Doch, denn IT-Sicherheit geht am besten wenn alle Bescheid wissen und alle mitmachen. Wirklich alle.

Sophos gibt eine Reihe von Ratschlägen wie in Unternehmen das Thema Sicherheit zur Selbstverständlichkeit für wirklich alle Mitarbeiter werden kann.

Wiesbaden, 21.10.2015 – Die Sicherheitskultur ist einer von mehreren Faktoren, die für Unternehmen von unschätzbarem Nutzen sein können. Keine noch so hohe Anzahl von Richtlinien oder technischer Kontrolle kann Sicherheitsverletzungen verhindern, wenn Firmen die Mitarbeiter nicht an ihrer Seite haben. Denn implementieren die IT-Manager Kontrollen, ohne sich um die Aufmerksamkeit, das Verständnis und die Kooperation der Arbeitnehmer zu bemühen, erreichen sie womöglich genau das Gegenteil. Ohne Bewusstsein für die Gefahren und mit einem fehlenden gegenseitigen Verständnis weichen Mitarbeiter auf alternative Lösungen aus und nutzen z.B. private E-Mails und File-Sharing-Dienste – eine Schatten-IT entsteht. Für die IT-Verantwortlichen sind Risiken aus diesen Technologien ungleich schwerer zu quantifizieren und noch schwerer zu adressieren.

Aber wie gelingt es am Besten, die Mitarbeiter zu einer Zusammenarbeit mit der IT-Abteilung zu bewegen und im Unternehmen eine Kultur der digitalen Sicherheit zu fördern?

1. Stellen Sie einen Bezug zum täglichen Leben her und: Alle Mann an Bord!
Während in den Medien die Cyberangriffe auf Staatsebene für Schlagzeilen sorgen, besteht für Organisationen eher die Gefahr, von einer kriminellen Vereinigung aufs Korn genommen zu werden. Es gibt einige erschreckende Statistiken dazu, wie viel eine Datenpanne betroffene Unternehmen kosten kann. Beispiele mit Finanzbezug können helfen, beispielsweise das Führungsteam an Bord zu holen und dessen Bewusstsein für den Ernst der Lage zu schärfen.

Möchten Unternehmen jedoch die Arbeitnehmer für die Gefahren sensibilisieren, ist es sinnvoller, die konkreten Bedrohungen für die jeweiligen Rollen und Tätigkeitsbereiche verständlich zu erklären. So wird beispielsweise die Finanzabteilung eher Interesse an einer Geschichte über den Missbrauch einer CEO Position zeigen, als sich für die Themen der Systemadministratoren zu erwärmen. Alle Mitarbeiter individuell abzuholen dauert natürlich ein wenig länger, hat jedoch wesentlich mehr Aussicht auf Erfolg. Noch wirkungsvoller ist es, den CFO selbst, etwa im Rahmen eines Teammeetings, das Thema Datensicherheit ansprechen zu lassen.

2. Halten Sie das Thema lebendig und relevant
Obwohl die andauernden Nachrichten über geschädigte Unternehmen auch bisweilen ermüdend wirken können, so helfen sie doch dabei, das Thema aktuell zu halten. Es ist nur eine Frage der Zeit, bevor die nächste Story über Datenmissbrauch oder eine Datenpanne erscheint. Nehmen Sie jede Gelegenheit wahr, um mit den Schlüsselpersonen im Gespräch zu bleiben. Richten Sie Keyword Alerts im Zusammenhang mit Ihrer Branche oder Region ein. Podcasts sind eine weitere gute Möglichkeit, um mit den neuesten Ereignissen Schritt zu halten. Bei Sophos mögen wir risky.biz – und unseren eigenen Chet Chat natürlich.

3. Machen Sie Werbung, attraktive Werbung
Marketing ist kein Gebiet, auch dem Sicherheitsverantwortliche üblicherweise glänzen. Informationsmaterial, das einen IT-Spezialisten anspricht, unterscheidet sich ganz sicher von dem, das die restlichen Mitarbeiter interessiert. Bitten Sie die Marketing-Abteilung, Ihnen behilflich zu sein. Lassen Sie Plakate, Aufkleber, Stress-Bälle oder anderes Material produzieren, das die Aufmerksamkeit der Mitarbeiter längerfristig aufs Thema lenkt und bleiben Sie dran. Einige Unternehmen setzen bereits spezielle Awareness-Programme ein, um auf Themen der Informationssicherheit hinzuweisen. Der Aufwand lohnt sich.

4. Messen Sie, was Sie können, teilen sie die Ergebnisse mit
Der Spruch "was gemessen wird, wird auch gemanagt" ist so wahr wie eh und je. Wenn Ihre Awareness-Kampagne sich beispielsweise mit dem Thema Phishing befasst, dann führen Sie regelmäßig Tests durch und überprüfen Sie, ob Verbesserungen erreicht wurden. Tests helfen Ihnen, die Effektivität Ihrer Kampagne und ihrer Materialien zu bewerten und sie unterstützen auch die Message selbst.

Seien Sie kreativ. Womöglich lassen sich die Ergebnisse noch schneller verbessern, wenn Sie ein „Naming and Shaming“ etablieren. Dabei müssen keinesfalls reale Personen an den Pranger gestellt werden. Die Nennung von Abteilungen, Divisionen oder Niederlassungen ist völlig ausreichend, um Aufmerksamkeit zu erregen. Veröffentlichen Sie die Listen und schicken Sie Süßigkeiten an die Gruppen mit den besten Ergebnisse und Info-Poster an die Tabellenletzten. Jede Aufmerksamkeit ist gut.

Falls solche Möglichkeiten intern nicht bestehen, können auch externe Dienstleister in Anspruch genommen werden. Aber bitte bedenken Sie: die wenigsten Arbeitnehmer gehen absichtlich Risiken oder setzen ihre eigene Firma einer Gefahr aus. Häufig sind fehlende Informationen der Grund für falsches Verhalten. Der kritische Punkt ist immer die Aufklärung – und die müssen Sie und Ihre Abteilung vor jedem Mitarbeitertest geleistet haben. Es ist schlicht nicht realistisch, dass die Arbeitnehmer einen Phishing-Versuch erkennen, ohne dass die IT ihnen jemals gezeigt hat, wie dieser aussieht.

5. Für Neuzugänge gilt: Gleich beim Jobantritt auf Nummer Sicherheit
Ein guter Start für die neuen Kollegen im Unternehmen zahlt sich auch für die IT-Sicherheit aus. Nun müssen diese an ihrem ersten Arbeitstag kein mehrstündiges Sicherheitstraining durchlaufen, aber es wäre sinnvoll, das Thema gleich prominent zu platzieren. Nutzen Sie auch hier jede Möglichkeit, die sich bietet. Gibt es ein Starter-Paket? Eine Onboarding-Präsentation? Stellen Sie sicher, dass das Thema IT-Sicherheit hier kurz und prägnant erklärt wird. Platzieren Sie eine Desktop-Verknüpfung zu Schulungsunterlagen auf dem Rechner der neuen Mitarbeiter oder ein kurzes Click-Through-Manual zu ihrer ersten Anmeldung. Auch hier gilt: messen Sie! Lassen Sie die Neuen nach 30 Tagen ein On-Boarding-Quiz durchführen und prüfen Sie, ob das nötige Wissen vorhanden ist.

6. Die „Broken Windows“ Theorie – seien Sie achtsam
Erstmals 1982 in einem Artikel der Sozialwissenschaftler James Q. Wilson und George L. Kelling vorgestellt besagt diese Theorie, dass eine hohe Aufmerksamkeit gegenüber kleinen Vergehen dazu führt, dass größere gar nicht erst entstehen.
Übertragen auf die IT-Sicherheit bedeutet dies: achten Sie auch auf Kleinigkeiten. Sehen Sie einen ungesicherten Computer? Gehen Sie nicht vorbei. Hören Sie, wie Mitarbeiter ihre Passwörter austauschen? Reagieren Sie.

Eine Kultur der Cybersicherheit können Sie kaum allein erschaffen – Sie brauchen Verbündete. Da sind ihre IT-Kollegen die erste Anlaufstelle. Aber auch Sicherheitsverantwortliche in anderen Abteilungen können hilfreich sein. Der Kollege in der Buchhaltung, der Ihnen jede Spam-E-Mail einzeln weiterleitet, mag zwar nerven, aber er ist Ihr Verbündeter und wird Sie bestimmt unterstützen, so gut er kann.

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt. Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:
Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de