Cybersecurity hatte einen blinden Fleck. Bis jetzt!

Herausforderung

Hacker sind heutzutage mehr Trickbetrüger als Nerds.

Statt Passwörter zu knacken und Viren zu versenden, geben Sie sich geschickt als Kollegen aus, provozieren übereilte Reaktionen oder verführen Teams dazu, Geheimnisse zu verraten.

Dazu nutzen Hacker die gesamte Klaviatur menschlicher Schwächen: sie erzeugen Stress und Ablenkungen, sie appellieren an Obrigkeitshörigkeit und Ehrgeiz, und sie nutzen Scham und Überheblichkeit aus.

Risiken entstehen immer weniger durch Technik, und immer mehr durch Verhalten.

Lösung

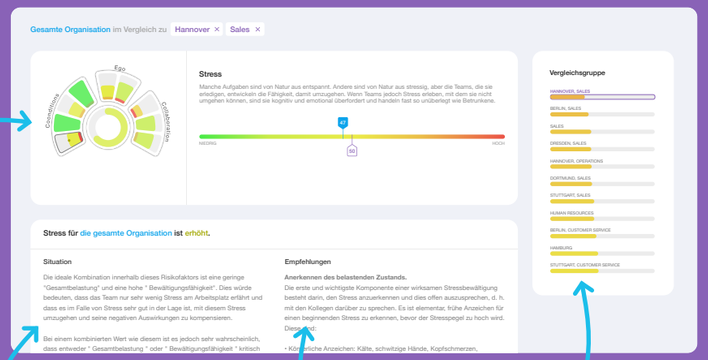
Branchen, in denen menschliches Fehlverhalten massiven Schaden anrichten kann, wissen schon seit Jahrzehnten, wie man risikoreiches Verhalten erkennt und verändert. In einem Maße, das Experten für Cybersicherheit noch nicht beherrschen.

Die dabei entscheidenden Risikofaktoren werden als das „Dirty Dozen“ bezeichnet. Sie stammen ursprünglich aus der Luftfahrt, finden aber überall dort Anwendung, wo es eine menschliche Risikokomponente gibt.

Die „Dirty Dozen“ werden seit Jahrzehnten erforscht und können mithilfe der Methoden der modernen Verhaltensforschung und quantitativen Soziologie, unserem Fachgebiet, erkannt und beeinflusst werden.

Alles verpackt in ein modernes und zugängliches Tool.

adair **misst und visualisiert Team-eigenschaften**, die für die Cybersecurity relevant sind ...



... **erklärt detailliert**, was sie bedeuten und welche Auswirkungen sie haben...

... und gibt dann **klare, pragmatische und hochwirksame Empfehlungen**, wie man Probleme lösen kann.

Und das **Team für Team.**

Das Dirty Dozen

Das Aussteuern dieser voll erforschten zwölf menschlichen Risikofaktoren bildet das Rückgrat der Alltagsabläufe fast aller Streitkräfte, der NASA, von Airbus, des NHS und der CDC. Sie waren eine zentrale Komponente im Umgang mit Covid-19.

Drei dieser zwölf Risikofaktoren (Wissen, Aufmerksamkeit und Ressourcen) werden in der Cybersicherheit bereits behandelt. Die bisher unberücksichtigten neun sind jedoch nicht minder entscheidend. adair ermöglicht es sie endlich auszusteuern.

Fehlendes **Wissen**

Fehlende **Aufmerksamkeit**

Unzureichende **Ressourcen**

adair zeigt sowohl das Problem als auch die Lösung auf

Auf Grundlage einer achtminütigen soziologischen Befragung berechnet adair für jedes Team in Ihrer Organisation die Wahrscheinlichkeit sicheren Verhaltens.

Es zeigt sowohl an, was das Problem ist, als auch was bewährte Mittel sind, sie zu mindern. Sie erhalten nicht nur eine schicke Kennzahl, sondern sehen auch, was Sie tun können, um die Lage zu verbessern.

Objektiv – zuverlässig – lösungsfokussiert.

Schlechte **Kommunikation**

Wenn Teams nicht ermutigt werden, frei zu sprechen oder Konsequenzen fürchten müssen, wenn sie sich offen mitteilen, werden wichtige Informationen unterschlagen. Anweisungen und Situationen werden unklar und interpretiert, wodurch eine leicht missbrauchbare Illusion von Einigkeit und Klarheit entsteht.

Selbstgefälligkeit

Selbstgefälligkeit ist ein wesentlicher Einflussfaktor für sicheres Verhalten, da sie entweder dazu führt, dass ein Fehler überhaupt nicht erkannt wird oder die Reaktion auf diesen unannehmbar langsam ist.

Ablenkung

Arbeitende Menschen denken voraus; die Wahrscheinlichkeit, ein paar Schritte zu überspringen, wenn man abgelenkt ist, ist sehr hoch. Eine gut getimte Ablenkung ist daher eines der wichtigsten Instrumente des Social Engineering.

Schlechte **Zusammenarbeit**

Wenn Ergebnisse in gemeinsamer Verantwortung liegen, hat eine uneindeutige Aufgabenteilung nicht nur massive Auswirkungen auf die Produktivität, sondern auch auf die Sicherheit: Hacker brauchen nur einen einzigen unbeaufsichtigten Prozessschritt, um Schaden anzurichten.

Erschöpfung

Erschöpfung ist wie Ersticken: Versäumte Erholung kann nicht einfach durch späteres mehr Ausruhen ausgeglichen werden. Ein übermüdetes Team ist nicht nur langsamer, sondern vor allem dümmer: Es ist nicht mehr fähig, grundlegende Fähigkeiten und Kenntnisse anzuwenden, ganz zu schweigen vom gesunden Menschenverstand.

Druck

Wenn der Druck, einen Termin einzuhalten, die Fähigkeit beeinträchtigt, Aufgaben korrekt auszuführen, wird ein sicheres Verhalten unmöglich. Kompromisse sind an der Tagesordnung, und Sicherheit rückt in der Prioritätenliste eines Teams immer weiter nach unten.

Fehlendes **Durchsetzungsvermögen**

Wenn Teams etwas Ungewöhnliches oder Irritierendes bemerken oder eine Schwäche entdecken, die niemand zu begreifen scheint, ist es nicht nur Aufgabe des Managements, sie anzuhören, sondern auch der Teams, ausreichend darauf aufmerksam zu machen.

Normen

Zahlreiche Prozesse laufen nicht so ab, wie sie konzipiert und implementiert wurden, sondern so, wie es sich im Alltag eingebürgert hat. Solch informelle Prozesse sind für Cybersicherheitsaudits in der Regel unsichtbar und stellen ein ernsthaftes Schlupfloch für Angriffe dar.

Stress

Manche Aufgaben sind von Natur aus entspannt. Andere sind von Natur aus stressig, aber die Teams, die sie erledigen, entwickeln die Fähigkeit, damit umzugehen. Wenn Teams jedoch Stress erleben, mit dem sie nicht umgehen können, sind sie kognitiv und emotional überfordert und handeln fast so unüberlegt wie Betrunkene.

www.adair.app
info@adair.app

adair GmbH
Zum Röthepfuhl 1
14974 Ludwigsfelde