1.

carmasec

security. done. right.

Interview mit Dr. Niklas Hellemann

Co-Gründer von SoSafe

In unserer Interviewreihe stellen wir Ihnen regelmäßig junge Teams und deren Produkte und Leistungen vor.

Das Kölner Unternehmen SoSafe, das sich 2018 gründete, fokussiert Cyberattacken auf Mitarbeiter von Organisationen und trainiert diese im Umgang mit solchen Bedrohungen. Dafür haben die drei Gründer, die mittlerweile 30 Mitarbeiter beschäftigen, eine Plattform geschaffen, die mittels regelmäßiger Bedrohungssimulationen Mitarbeiter für reale Angriffe sensibilisiert.

In dem Interview mit Dr. Niklas Hellemann sprechen wir über die Gründung von SoSafe, das Produkt und seine Hintergründe sowie Einsatzmöglichkeiten und Erfolge der Awareness Trainingsplattform.

1. Wie ist die SoSafe entstanden, was war die Initialzündung?

Dr. Niklas Hellemann, SoSafe

Wir hatten uns alle drei unabhängig voneinander schon länger mit dem Thema IT-Sicherheit beschäftigt. Teilweise waren das erste Erfahrungen als „Script Kiddy“ in der Jugend, in denen wir erste harmlose Versuche im Social-Engineering-Bereich gemacht haben. Teilweise aber auch auf wissenschaftlicher Ebene. So fand ich in meinem Psychologiestudium die Mechanismen der „Persuasion“, also die Überzeugung von Menschen bis hin zur Manipulation, immer schon extrem spannend. Die Initialzündung für SoSafe kam aber durch zwei konkrete Fälle in unserem Bekanntenkreis, bei denen zum einen eine ältere Dame mit einer Abwandlung des „Enkeltricks“ und ein Unternehmen durch eine ganz simple Phishing-Kampagne betrogen wurden. Wir haben uns dann die bisherigen verfügbaren Lösungen im Markt angesehen und waren in Punkto Didaktik und Qualität der Vermittlung nicht sehr überzeugt. Als Reaktion darauf haben wir den Entschluss gefasst, Awareness endlich einmal aus der trockenen Ecke herauszuholen und IT-Sicherheit auf „coole“ Art und Weise zu vermitteln.

2. Die persönlichen Hintergründe in den Vitas sind sehr unterschiedlich. Wie hat sich das Gründerteam gefunden und was waren bislang die größten Herausforderungen im Team?

Wir drei hatten zueinander durch ein kleines Projekt im Bereich des betrieblichen Gesundheitsmanagement gefunden, eigentlich ganz ohne Gründerromantik durch einen gemeinsamen Bekannten. Die verschiedenen Hintergründe und Lebensläufe wurden uns aber sehr schnell als klarer Vorteil bewusst. Neben den klaren Unterschieden auf dem Papier – ein Full-Stack-Entwickler, ein BWLer und ein Psychologe – bringen wir auch unterschiedliche Facetten in anderen Bereichen mit ins Team. Beispielsweise habe ich einen starken Fokus auf eine einfache und ästhetische UX/UI, während Felix und Lukas eine sehr pragmatische Herangehensweise an die Produktentwicklung haben. Beide Pole sind wichtig und sorgen für einen wettbewerbsfähigen Entwicklungsprozess.

Die größte Herausforderung bisher war sicherlich die Skalierung von einem Team aus drei Personen auf ein kleines Unternehmen von über 30. Während man in der Frühphase ja alles selber macht, muss man dann schnell auch abgeben lernen – vorausgesetzt, man kann ein starkes Team aufbauen. Glücklicherweise ist uns das gelungen und wir konnten Top-Profile anziehen, z.B. einen Ex-Kollegen von der Boston Consulting Group und Entwickler mit Security-Fokus.

3. Vor einigen Jahren waren Awareness-Maßnahmen bei Kunden regelmäßig Streichkandidaten und es wurde eher in technische statt in organisatorische Maßnahmen investiert - wenn überhaupt. Wie argumentiert ihr bei solchen Kunden, dass es sinn- und wirkungsvoller ist, sich auf den Faktor menschliches Bewusstsein zu fokussieren?

Ja, das ist ganz spannend – wir nehmen ein starkes Umdenken bei den CISO und ISBs von Unternehmen wahr. In der Vergangenheit herrschte ein unglaublicher Technikfokus vor, z.B. in dem man komplett auf Spamfilter oder Endpoint-Protection vertraut hat. Es ist natürlich auch sehr verlockend, einfach eine Filterlösung oder ein Secure-E-Mail-Gateway anzuschalten und damit ist alles gelöst.
Spätestens seit Emotet ist mit der Denke aber Schluss. Jede neue Phishing-Welle bleibt für eine gewisse Zeit unerkannt und viele Phishing-Kampagnen kommen ja komplett ohne Malware aus. Dahinter bleibt der Mensch als letzte Verteidigungslinie, was auch die Verantwortlichen erkannt haben. Wir argumentieren aber auch überhaupt nicht gegen technische Maßnahmen (was auch fatal wäre), sondern empfehlen schlichtweg die aktuell größte Lücke zu schließen und die Mitarbeiter abzuholen. Eine zeitgemäße Sicherheitsstrategie muss letztlich mehrere Schichten haben und das umfasst eben auch Schicht 8, den User.

4. Euer Ansatz adressiert das Themenspektrum menschliche Sensibilisierung sehr umfassend – von Phishing-Tests bis hin zu systematischen Schulungsangeboten für Unternehmen. Wie bewertet ihr die Resonanz eurer Leistungen? Greifen Kunden eher zur umfassenden Gesamtstrategie oder werden überwiegend einzelne Leistungen angefragt?

Da sehen wir ein ziemlich klares Bild: Die mit Abstand meisten Unternehmen – egal welcher Größe oder Industrie – präferieren eine Rundum-Sorglos-Lösung, die ihre Mitarbeiter das ganze Jahr mit verschiedenen Formaten „bespielt“. Das ähnelt auch ein wenig dem Wunsch, die „menschliche Firewall anzuknipsen“ – genau wie eine echte Firewall. Das bilden wir dann auch gerne ab, indem wir unsere Plattform noch mit einem zusätzlichen Service-Baustein verknüpfen, bei dem unser Expertenteam zielgerichtete Angriffe auf das Unternehmen konzipiert. So erhalten unsere Kunden dann eine echte „Fire-and-Forget“-Lösung, die mit wenig internem Einsatz sichtbare Effekte erzielt.

5. Ein zentraler Aspekt eures Leistungsangebots ist die psychologische und didaktische Ebene. Das unterscheidet euch sicherlich von vielen anderen Mitbewerbern. Würdet ihr das als Alleinstellungsmerkmal bezeichnen oder macht es das eher schwieriger bei der Positionierung eurer Leistungen?

Ich würde ganz klar sagen, dass das von den Kunden als absoluter Mehrwert gesehen wird. Einige unserer Kunden haben zum Beispiel schon einmal einen kurzfristigen „Phishing-Test“ durchgeführt und wundern sich, warum die Klickrate beim wiederholten Test nach einiger Zeit immer noch so schlecht ist.
Wenn sie dann unsere Lösung ausrollen, sind sie häufig überrascht über den starken Sensibilisierungseffekt. Diesen Effekt erreichen wir eben auch durch den starken Fokus auf die Didaktik, indem wir auf einer differenzierten Lernseite dem Mitarbeiter genau erklären, wie er die Mail hätte erkennen können, auf die er gerade hereingefallen ist. Er lernt also quasi live im Mailprogramm.
Daneben zeigen wir unseren Kunden dann auch in einem Analyse-Dashboard, auf welche psychologischen Taktiken z.B. bestimmte Abteilungen besonders anfällig sind. Dadurch können auch nicht-technische Mitarbeiter bei einer Folgekommunikation direkt einen Anknüpfungspunkt herstellen.

6. Die Sensibilisierung von Mitarbeitern für Sicherheitsrisiken ist grundsätzlich ein branchenneutrales Thema und auch weitgehend unabhängig von der Unternehmensgröße. Haben sich aus eurer bisherigen Erfahrung dennoch herausgestellt, dass die Nachfrage aus einigen Branchen besonders hoch ist oder eure Dienstleistungen besonders gut passen?

Dr. Niklas Hellemann, Gründer von SoSafe, als Referent auf den ISD 2019

Sicherlich hat die KRITIS-Verordnung in den entsprechenden Sektoren, wie dem Gesundheitswesen oder bei Versorgern, für Dynamik gesorgt. Hier beobachten wir infolgedessen, dass viele Organisationen z.B. ein ISMS einführen oder eine ISO-Zertifizierung angehen. Das bringt dann natürlich auch direkt die Frage nach den Trainings- und Awareness-Maßnahmen mit sich (die die ISO ja auch klar vorschreibt). Wir haben daher viele Stadtwerke oder größere Kliniken als Kunden, die unsere Lösung im Zuge dessen ausrollen. Auch da wir ein spezielles ISO-Reporting bieten, das den Entscheidern beim Schulungs-Nachweis Arbeit abnimmt.
Davon abgesehen, würde ich aber sagen, dass das Thema Awareness für alle Branchen und Unternehmensgrößen gleichermaßen drängend ist.

7. Ihr bietet neben Adhoc-Maßnahmen wie Phishing-Tests auch eine kontinuierliche Erfolgsmessung eurer Maßnahmen an. Wie ist da bislang die Resonanz bei euren Kunden?

Man muss hier klar sagen, dass der Großteil unserer Kunden unsere Lösungen langfristig einsetzt. Kurzfristige Maßnahmen, wie Phishing-Tests, setzen wir eher ein, wenn es akut Bedarf gibt oder auch um das Ausmaß des Problems zu bemessen, z.B. gegenüber der Geschäftsführung.
Hintergrund ist eben auch, dass wir die Phishing-Simulation primär als Lerntool und nicht als Testtool sehen. Natürlich ist es sehr spannend herauszufinden, auf welche Taktiken meine Führungskräfte besonders gut hereinfallen. Das Schöne an unserem dauerhaften Konzept ist es aber, dass wir den Gefährdungsgrad auch nachhaltig verringern können, wenn man Simulation und E-Learning gemeinsam und dauerhaft einsetzt.

8. Die Digitalisierung treibt speziell den Mittelstand gerade dahin, sich mit neuen Technologien auseinanderzusetzen. Stellt ihr bereits fest, dass dort ein damit einhergehend auch ein erhöhtes Sicherheits- und Risikobewusstsein einhergeht?

Das wäre schön, wenn mit steigendem Digitalisierungsgrad auch automatisch ein höheres Sicherheitsbewusstsein käme! Leider bin ich aber eher der Auffassung, dass der Treiber für Letzteres schlichtweg der schiere Schmerz bzw. die Angst davor ist. Spektakuläre Fälle wie der des Automobilzulieferers Leoni, der im Rahmen eines Phishing-Angriffs 40 Mio. EUR an einen Betrüger überwiesen hat, führen hier eher dazu, dass umgedacht wird. Wir haben nun allerdings auch eine Frequenz an Angriffen erreicht, bei der es kaum mehr eine Branche ohne eines dieser abschreckenden Beispiele gibt. Daher glaube ich auch, dass immer mehr Unternehmen auch den Weg hin zur Prävention gehen und sich ausreichend absichern, bevor es sehr viel teurer wird.