carmasec

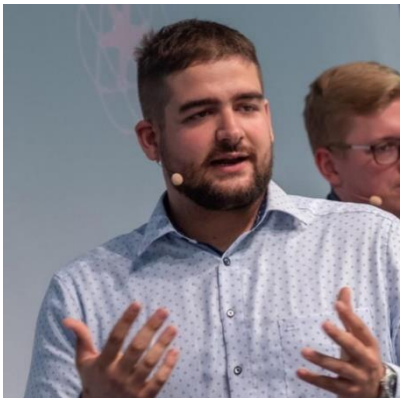
security. done. right.

Interview mit Matteo Cagnazza

Co-Gründer von Aware7

Im Rahmen unserer Mentorships für Nachwuchskräfte unterstützen wir junge Startups auf ihrem Weg von der innovativen Idee zum marktreifen Produkt. In einer Interviewreihe möchten wir Ihnen drei Unternehmen, deren Gründer und kreative Ideen uns überzeugt haben, vorstellen. Das Cybersicherheits-Startup Aware7 hat es sich zur Aufgabe gemacht, menschliche und technische Sicherheitslücken zu finden und aufzuzeigen. Mit Events wie Live Hackings, Penetrationstests oder Schulungen touren sie mittlerweile durch ganz Europa und sensibilisieren für Schwachstellen in IT-Systemen von Unternehmen. Das Interview haben wir mit dem Co-Gründer Matteo Cagnazzo geführt.

1. Ihr seid viel im Namen der Cybersicherheit unterwegs und tourt mit Live-Hackings und Awareness-Aktivitäten quer durch das Bundesgebiet und teilweise auch darüber hinaus. Habt ihr überhaupt noch einen Überblick, wie viele Veranstaltungen ihr bislang gemacht habt?



Matteo Cagnazzo, Co-Gründer Aware7

Das ist richtig. Wir sind mittlerweile sogar europaweit unterwegs. Wir waren in der Schweiz, im Baltikum und den Benelux-Ländern. In 2018 haben wir mehr als 200 Veranstaltungen durchgeführt. Diese Marke haben wir in diesem Jahr bereits überschritten. Wir verdoppeln unser Pensum also und haben noch nicht vor aufzuhören.

2. Wie schätzt ihr den IT-Sicherheitsmarkt und die Nachfrage ein? Seht ihr noch eine Chance, den Kampf gegen Cyberkriminalität zu gewinnen?

Der IT-Sicherheitsmarkt ist meiner Meinung nach zurzeit sehr stark. Wir sehen eine wachsende Nachfrage, was sicherlich auch mit verabschiedeten Gesetzen wie der DSGVO oder der KRITIS-Verordnung zusammenhängt. “Den Kampf zu gewinnen” ist meiner Meinung nach aufgrund der Asymmetrie zwischen Angreifern und Verteidigern nicht die richtige Formulierung. Ich denke, dass wir bei der Erkennung von Cyberangriffen und Betrugsmaschen noch deutliches Potential haben. Komplett gewinnen können wir Verteidiger diesen Kampf aber nicht. Ziel ist es, der Gegenseite immer einen Schritt voraus zu sein.

3. An wen richtet sich euer Angebot – ihr seid ja sowohl bei privat-wirtschaftlichen Unternehmen im Einsatz als auch bei öffentlichen und gemeinnützigen Einrichtungen?

Unsere Awareness-Vorträge und -Schulungen richten sich tatsächlich an alle Zielgruppen. Einzige Voraussetzung für dieses Angebot ist das Interesse an IT. Die Veranstaltungen zu den Themen Pentesting und Phishing sprechen dagegen deutlich den privat-wirtschaftlichen Bereich an. Aktuell entwickeln wir mehrere Technologien, die wir gezielt in Richtung kleiner und mittlerer Unternehmen (KMUs) adressieren.

4. Wie sieht euer Leistungsangebot aus? Mit einmaligen Veranstaltungen lässt sich Awareness mittel- bis langfristig nicht erreichen und Angriffsszenarien wie „Spear Phishing“ oder auch „CEO Fraud“ funktionieren aus Perspektive der Angreifer leider sehr gut. Wie sieht eure Antwort darauf aus?

Eine einzelne Veranstaltung kann höchstens als Impuls oder als Auffrischung gesehen werden. Viele KMUs empfinden unsere Angebote als Weckruf und setzen sich nach einem unserer Workshops mit dem Thema Cyber Security stärker auseinander. Bei Unternehmen, die aus Cybersecurity-Sicht größer oder reifer sind, sind unsere Veranstaltungen meist in eine weiter gefasste Security-Kampagne, eine Zertifizierung oder in das Programm eines IT-Sicherheitstags eingebettet. Perspektivisch müssen wir Cyber Security als holistisches Gesamtkonzept betrachten. Die beste Kryptographie schützt uns nicht, wenn wir Mitarbeiter nicht schulen, Risiken zu erkennen. Genauso können aber auch Mitarbeiter nicht zur Verantwortung gezogen werden, wenn innerhalb eines Unternehmens keine BackUp-Lösung implementiert oder getestet ist.

5. Sieht euer Angebot auch vor, Kunden regelmäßig und nicht nur einmalig zu besuchen und dort Workshops zu halten, um nachhaltige Effekte für die Awareness zu erzielen? Kann man euch beispielsweise auch für jährlich-, halbjährliche oder quartalsweise Workshops zu diesen Themen buchen?

Ja, das ist möglich - dann ist Live-Hacking beispielsweise das Kick-Off Event. Wir bieten unterschiedliche Konzepte an, von der Integration in eine bestehende Awareness-Kampagne bis hin zur Planung und Durchführung einer Kampagne “from scratch” mit individuellen Workshops und Inhalten.

6. Ihr seid momentan mit eurem Projektgeschäft sehr erfolgreich und viel unterwegs. Parallel dazu läuft aber auch die Weiterentwicklung eures Produkts. Könnt ihr kurz die Leistungen eurer Plattformlösung skizzieren? Und wann wird sie voraussichtlich verfügbar sein?

Risikoanalyse ist nicht leicht, besonders für KMUs. Für die Erhöhung der Resilienz ist es aber wichtig zu wissen, an welcher Stelle der größte Handlungsbedarf besteht und wie dieser kosteneffizient bedient werden kann. Die von uns entwickelte Plattform hilft, technische und menschliche Sicherheitslücken aufzudecken und mit geringem Budget zu schließen. Die entwickelte Plattform ermöglicht die Ermittlung des Angriffspotentials durch die Mitarbeiter und Technologie. Weiterhin unterstützt die Plattform Unternehmen bei der individuellen Auswahl von Gegen- und Schulungsmaßnahmen. Hierzu werden vierteljährliche, monatliche oder zeitlich-individuelle Reports erstellt, mit deren Hilfe Aussagen über die Wirksamkeit von empfohlenen Maßnahmen hinsichtlich der Angriffsfläche Mensch getroffen werden können. Dies ist eine bisher nicht quantifiziert messbare Größe. Die Erkenntnisse können in weitere individuelle Maßnahmen zur Risikominimierung einfließen. Wir planen noch im Laufe dieses Jahres eine geschlossene Beta-Phase.

7. Mit dem Thema Awareness fokussiert ihr euch sehr stark auf die menschlichen Aspekte in der Cybersicherheit. Der Mitarbeiter ist häufig nicht nur der schwächste Faktor, weil er nicht gegen IT-Risiken und professionelle Cyberangriffe sensibilisiert ist, sondern auch weil von Unternehmensseite eher technische Schutzmaßnahmen priorisiert werden. Wie geht ihr damit um?

Unserer Meinung nach ist es stets das Zusammenspiel von Mensch und Technik. Cyber Security muss holistisch betrachtet werden. Nur unter Beachtung menschlicher, technischer und organisatorischer Aspekte kann eine Erhöhung der Resilienz eines Unternehmens stattfinden. Daher entwickeln wir die Plattform, um Unternehmen eine Möglichkeit zu geben, das Thema Cyber Security ganzheitlich zu betrachten.

8. Neben Unternehmenskunden vermittelt ihr auch Schülern ein Sicherheitsbewusstsein und habt mit cyberpflege.de auch ein Hilfsmittel für die Abmeldung aus sozialen Medien geschaffen. Wie ist eure Einschätzung beim Themenbereich Datenschutz, Datensparsamkeit und (sozialer) Medienkompetenz gerade bei dieser Zielgruppe? Sind wir schon in einer „Post-Privacy-Ära“?

Matteo Cagnazzo und Chris Wojzechowski, Aware7

Schüler*innen sind tatsächlich in Bezug auf Datenschutz oft kritisch eingestellt. Den echten Namen oder die Adresse an Dritte weiterzugeben, wird hinterfragt. Allerdings fehlt häufig ein technisches Verständnis. Snapchat sehen viele beispielsweise als unkritisch, da die Datei vom Smartphone des anderen verschwindet. Das ist natürlich nicht ganz zu Ende gedacht, da Daten zwischendurch auf Servern zwischengespeichert werden. Die weitere Verarbeitung der Daten ist hierbei nicht geklärt. Selbst wenn die miteinander kommunizierenden Handys direkt nebeneinander liegen, können Daten einmal um die halbe Welt gehen. Bevor also über “Post-Privacy” oder eine junge Generation, die den Datenschutz über Bord wirft, diskutiert wird, sollten wir erstmal entsprechendes Verständnis und Wissen erzeugen. Nur so kann jeder - egal ob jung oder alt - die Bedeutung von Informationen, das Teilen mit Dritten und inwieweit sie unseren Handlungsspielraum erweitern oder einschränken, bewerten.

9. Wenn ihr ganz generisch einen Wunsch für konkrete Maßnahmenumsetzung bei euren Kunden frei hättet: Was würdet ihr im Sinne der besseren Gefahrenabwehr von Cyberangriffen wählen?

Dass der Kunde vorab weiß, wo seine Probleme liegen und entsprechend zielgerichtet Maßnahmen einkaufen kann oder entsprechend individuelle Inhalte für Awareness-Maßnahmen definieren kann. Oft ist gerade das Erstellen der Inhalte für Awareness-Kampagnen eher “Fischen im Trüben”. Es ist nicht richtig klar, wo denn der Schuh bei den Mitarbeitern oder im Unternehmen wirklich drückt.