Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur

Band: 103 (2023)

Heft: 1111

Rubrik: Das Unternehmergespräch

DAS UNTERNEHMERGESPRÄCH

«Betrug wird immer besser und raffinierter»

Als Mitgründerin von Futurae ist Sandra Tobler darauf spezialisiert, Login-Anforderungen für digitale Portale so sicher zu machen, dass Hacker oder Betrüger sie nicht knacken können. «Aber Fingerabdrücke sind doch bestimmt eine sehr sichere Methode, um sich bei einem Geräte- oder Online-Dienst anzumelden», fordere ich sie heraus, nachdem ich an meinem Glas Wasser genippt habe. «Fingerabdrücke? Ich habe doch jetzt deine Fingerabdrücke...», antwortet Tobler und starrt auf mein Glas. Wir lachen beide – und ich wünschte mir Handschuhe herbei.

Das Cybersicherheitsunternehmen Futurae ist in Zürich praktisch neben dem Bahnhof Giesshübel angesiedelt und bietet seinen Kunden Betrugserkennung und eine starke Authentisierung, die auf verschiedenen Kriterien, zum Beispiel Multifaktor, basiert. Zu den 125 Kunden zählen Barclays, Santander, viele Schweizer Kantonalbanken, Börsen, Migros, Versicherungen, Spitäler und mehr. «Früher brauchte man nur einen Anmeldenamen und ein Passwort, um auf sein Konto zuzugreifen – aber Passwörter kann man knacken, wenn man genug Zeit hat», erklärt Tobler. Futurae biete einen Service, bei dem die Anmeldung bei einer Plattform mehrere Authentifizierungsschritte erfordere. So müsste man neben einem Passwort auch eine oder mehrere persönliche Informationen eingeben. Biometrische Daten, die sich auf einzigartige körperliche Merkmale beziehen, geben Auskunft darüber, wer man ist. Kontrollfragen wie der Name des ersten Haustiers beziehen sich darauf, was man weiss. Ein zusätzliches elektronisches Gerät ist ein Beispiel dafür, was man besitzt.

Ähnlich wie das Militär befindet sich die Branche in einem ständigen Wettlauf zwischen Massnahmen und Gegenmassnahmen. So wie jeder Panzer mit neuen Methoden der Panzerabwehr neutralisiert werden kann, finden Kriminelle ständig neue Wege, um modernste Authentifizierungsmassnahmen zu durchdringen. Deswegen ist Futurae daran, sogenannte kontextbasierte Sicherheitsmethoden zu erforschen.

Sandra Tobler
illustriert von Dunvek.

Firma
Futurae Technologies AG

Position
Verwaltungsratspräsidentin & Chief Customer Officer

Firmensitz
Zürich

Branche
Cybersecurity

Das läuft so: Loggt man sich auf dem Computer in der Regel im Beisein des eigenen Smartphones oder der Smartwatch in sein Bankkonto ein, wird dieses Verhaltensmuster von Futurae registriert. Befinden sich dann bei einem Login-Versuch hingegen keine solchen persönlichen Geräte in der Nähe, stellt die Software eine Anomalie fest. In diesem Fall kann die Anmeldung verweigert werden, oder es werden weitere Informationen angefordert, bevor eine erfolgreiche Anmeldung möglich ist. Logins sind bei Futurae immer anonym, da «wir zu keinem Zeitpunkt wissen, wer der Kunde unseres Kunden ist». Futurae ist sich bewusst, dass der beste Weg, die wichtigsten Daten der Kunden zu schützen, darin besteht, diese Daten gar nicht erst zu besitzen.

Bevor sie mit Futurae startete, arbeitete Tobler in San Francisco für das Eidgenössische Departement für auswärtige Angelegenheiten EDA. Doch die Privatwirtschaft reizte sie mehr. «Ich bin ein unternehmerischer Mensch und geniesse es, selbst etwas aufzubauen, zusammen mit Menschen, die im gleichen Tempo arbeiten und gleichgesinnt sind.» So gründete sie 2016 Futurae zusammen mit Claudio Marforio und Nikos Karapanos und hatte damit so viel Erfolg, dass sie derzeit 47 Mitarbeiter beschäftigen kann. Drei Viertel davon sind Programmierer, darunter Sicherheitsingenieure und ein Team für künstliche Intelligenz.

Futurae denkt, ganz dem Firmennamen verpflichtet, ständig voraus, um zu antizipieren, wie Hacker in Zukunft arbeiten werden. Dieses Denken spiegelt sich poetisch in der Tatsache wider, dass Tobler eine Woche vor meinem Treffen als CEO zurücktrat und Chief Customer Officer wurde, weil sie die Kundenseite mehr schätzt und glaubt, dass dies der beste Weg sei, um die Entwicklungen zu verstehen. «Betrug wird immer besser und raffinierter, weil fortschrittliche Tools durch KI den Hackern das Leben leichter machen», lautet ihre Prognose. Es sieht so aus, als hätte Tobler auch künftig alle Hände voll zu tun. Ob sie sich dabei auch Handschuhe anziehen wird? (as) ‹