

Digitale Angriffe aktiv abwehren

Friedrich Kisters ist CEO der Kreuzlinger OriginStamp AG, Marktführerin für Blockchain-basierte digitale Zeitstempel. Kisters neuester Clou: die «TrustedBox». Mit ihr lassen sich Daten automatisiert, verschlüsselt und digital gestempelt sichern. Hacker haben so keine Chance mehr, aus gestohlenen Daten Profit zu schlagen. Im Gespräch erklärt Kisters, warum gerade Schweizer KMU attraktiv für digitale Angriffe sind und wie sie diese einfach abwehren können.



Friedrich Kisters, was muss ein KMU heute tun, um in Sachen Datensicherheit smart zu sein?

Sie sollten in Sachen Datensicherheit ähnlich pragmatisch vorgehen wie beim Autokauf: Ein einfacher Wagen mit cleverem Tuning kann viel Geld sparen. Unsere TrustedBox benutzt als Hardware einen handelsüblichen Network-attached-Storage-Dateiserver (NAS), wie Sie ihn in jedem Interdiscount kaufen und dann als Backup einsetzen können. Im Fall einer Ransomware-Attacke ist Ihre Sicherheit allerdings nahe null. Wir «tunen» diese NAS softwareseitig auf eine sehr hohe Sicherheit. Einmal installiert, erledigt die TrustedBox die Datensicherungen im Hintergrund.

«Die Schweiz als reiches Land ist für solche Attacken besonders beliebt.»

Und wie genau machen Sie das?

Sie können Daten von allen Ihren Mitarbeitern lokal verschlüsseln und dann direkt auf die TrustedBox vor Ort speichern. So haben Sie immer eine aktuelle Version der Daten, falls einem Mitarbeiter das Notebook abhandenkommt. Von jetzt an läuft alles automatisch im Hintergrund: Die TrustedBox erstellt ein tägliches Backup aller hinzugekommenen Daten und verschlüsselt diese erneut. Dann erstellt sie zu jeder einzelnen Datei einen Blockchain-basierten Zeitstempel, der zweifelsfrei dokumentiert, dass diese Daten in dieser Form zu diesem Zeitpunkt existiert haben.

Die Echtheit des Inhaltes jeder Datei ist damit mathematisch nachrechenbar?

Ja, und unlöschar in der Blockchain verankert. Schauen Sie Ihre Daten als Boote an: Jetzt hat jedes Boot einen festen Anker. Dann werden diese doppelt verschlüsselten Daten auf Amazon-Webservices datenschutzkonform gesichert, noch

mals verschlüsselt und eingefroren, solange Sie wollen. Jetzt haben Sie ein dreifach verschlüsseltes tägliches Archiv Ihrer Daten in einer der weltweit sichersten Clouds unveränderbar gesichert – und zu jeder Datei einen Ursprungs- und Echtheitsstempel in der Blockchain.

Wie viele Daten kann eine TrustedBox speichern – und was kostet sie?

Die kleinste Variante erlaubt bis zu sechs Terabyte Daten, was für viele KMU genügt. Beim ersten Backup sind bis zu sechs Millionen Daten-Zeitstempel kostenlos dabei ... Hinzu kommt das Abo für die monatlichen Zeitstempel und das Einfrieren der Daten. Das kleinste Jahrespaket inklusive Hardware und Abos kostet 8700 Franken. In den Folgejahren liegen die Abokosten nur noch bei etwa 300 Franken im Monat. Sie finden keine vergleichbare Lösung unter 10'000 Franken!

Und wie schützt die TrustedBox vor einer Ransomware-Attacke?

Eine Ransomware-Attacke kann daran erkannt werden, dass sich wegen des Verschlüsseln der Daten durch den Angreifer plötzlich viele Daten ändern und somit auch die Anzahl Blockchain-basierter Zeitstempel in die Höhe schießt. Das löst einen Alarm wie bei einem Tsunami aus, und wir können den Kunden umgehend warnen. Er muss im Idealfall nur die Daten eines Tages löschen und wiederherstellen lassen, um das Problem zu lösen.

Alle Daten sind ja unlöschar vorhanden ...

... und werden täglich versioniert archiviert, genau! Sie können also jederzeit wiederhergestellt werden. Jede Datei besitzt einen mathematischen Beweis ihres Ursprungszeitpunktes und Inhalts. Es ist kaum mehr möglich, unbemerkt die Metadaten zu ändern. Bei jeder Änderung erstellt die TrustedBox einen neuen Zeitstempel als Beweis. Sollte ein Angreifer Daten gestohlen haben, kann einfach nachgewiesen werden, dass man sie zum Speicherzeitpunkt tatsächlich bereits besessen hat. Jeder, der diese Daten danach ohne Erlaubnis verkauft, kauft oder besitzt, macht sich potenziell strafbar. Die Daten sind also schwerer verkäuflich, da der Zeitstempel jederzeit überprüfbar ist.

Gibt es eine eigentliche Strategie hinter der TrustedBox, um KMU zu helfen?

Ja – und diese ist dringend notwendig! Wir leben in der Schweiz besser als der Rest der Welt und sind deshalb ein beliebtes Ziel, leider auch für digitale Angriffe. Deshalb hat sich der Verein Smarter Thurgau die Sicherheit als zentrales Thema ausgesucht, um das Vertrauen im Umgang mit Daten zu stärken. Gemeinsam – **die OriginStamp AG ist Technologiepartner des VST** – wollen wir, dass alle KMU die Möglichkeit bekommen, digital souverän zu werden, um Angriffe von aussen auch digital abwehren zu können. Die TrustedBox ist ein erster wichtiger Schritt zu dieser Grundabsicherung.

Und welche weiteren Schritte sind geplant?

Wir wollen eine «Lost Data Registry» aufbauen, wo jedes KMU Daten hinschicken kann, von denen es vermutet, dass sie jemand unberechtigt kopiert hat. Wir planen, gemeinsam eine Suchmaschine einzurichten, die das Internet permanent nach solchen Daten durchsucht. Sobald etwas gefunden wird, kann die Löschung verlangt oder rechtlich gegen die Verbreitung vorgegangen werden. Und im geplanten

Digital Campus Thurgau soll ein Kompetenzzentrum zum Thema Sicherheit & Vertrauen entstehen – ein neues Zentrum für digitale Sicherheit. Das könnte die Region auch als digitalen Standort massiv aufwerten. Besonders interessant ist dabei die Verbindung der digitalen mit der realen Welt, also des realen Vertrauens mit der digitalen Sicherheit. Diese fehlt heute völlig.

Zurück zur TrustedBox. Gibt es schon Firmen, die sie einsetzen?

Natürlich – folgende KMU darf ich namentlich nennen: Die Immokanzlei AG in Kreuzlingen, deren CEO Attila Wohlrab auch Präsident des AGV ist, die BPA Treuhand AG mit CEO Lorenz Zwahlen in Frauenfeld, die Ganten Trustees Ltd. mit CEO Klaus Stark in Liechtenstein und die von Büren + Sommer AG mit CEO Roland von Büren in Berg, ein Thurgauer Handwerksbetrieb, spezialisiert auf Innenausbau aus Holz, Brandschutz und Einbruchschutz.

«Schauen Sie Ihre Daten als Boote an: Jetzt hat jedes Boot einen festen Anker.»

Und wieso interessiert sich eine Manufaktur für die TrustedBox?

Fast alle Handwerksbetriebe sind heute auch digital unterwegs. Und es ist für den Geschäftsführer mühsam, ständig Magnetbänder mit archivierten Daten aktualisieren zu müssen. Die TrustedBox erledigt das. Eingesparte Zeit und zusätzliche Sicherheit sind schlagende Argumente für Praktiker, die sich nicht gerne mit digitalen Problemen herumschlagen.

Sind Ransomware Attacken für Schweizer KMU überhaupt eine Gefahr?

Oh ja! Es gibt seit kurzer Zeit Plattformen krimineller Organisationen, die alles zur Verfügung stellen, was es für eine Ransomware-Attacke braucht – «Ransomware as a Service», sozusagen. Investiert dort jemand Geld, wird damit eine Verschlüsselungsattacke ausgeführt. Im Erfolgsfall zahlt das betroffene KMU Lösegeld für die Entschlüsselung seiner Daten – und der «Investor» erhält von der RaaS-Plattform das Vielfache seiner Investition zurück. Die Schweiz als reiches Land ist für solche Attacken besonders beliebt. Wer sich jetzt nicht schützt, handelt schlicht fahrlässig.

Sie finden die TrustedBox unter trustedbox.originstamp.com. Friedrich Kisters erreichen Sie via Mail (trustedbox@originstamp.com) oder Telefon (+41 71 577 02 70). Allen LEADER-Lesern offeriert OriginStamp von August bis Oktober 2020 einen **KMU-Rabatt von sieben Prozent** auf das Jahrespaket. Es kostet somit nur 8091 Franken. Der Rabattcode lautet: LEADER.