Übersetzung zum Interview im Rahmen des Cyberkongress 2020 mit Chris Bailey und Daniel Kinlock

1:06
Chris – Du bist ein Pionier in Sachen Zertifizierung. Stellst Du Dich bitte vor?

1:15
Sicher, ich bin im Bereich der Autorisierung von Zertifikaten seit 20 Jahren tätig. In dieser Zeit habe ich die DV Zertifikate (Domain Validated) miterfunden, die heute einen Grossteil des Internetverkehrs mit SSL / TSL verschlüsseln. Ich bin aber auch einer der Co-Erfinder fuer die Extended Validated Zertifikate, welche die höchste Authentisierung von Identitäts Zertifikaten auf dem Markt heut zutage sind. Des weiteren bin ich auch einer der Gruender des sogenannten CA Browser Forums. Das ist die Organisation, die managt, wie CA's (Certificate Authorizations) und die Browser miteinander agieren. Ich bin auch einer der Gruender des CA Security Counsil. Diese Organisation empfiehlt weltweit die Standards für diese Industrie.

9:51
Was ist die Rolle von TLS-Zertifikaten? Chris, kannst Du uns Beispiele für einige kürzlich erfolge Zertifkats- und damit Service-Ausfälle geben?

10:10
Klar Daniel, also einfach gesprochen, wenn wir uns über Zertifikatsausfälle unterhalten dann reden wir eigentlich darüber, dass ein TLS Zertifkate aufgehoert hat zu funktionieren. Meistens ist das TLS Zertifikate ausgelaufen oder verfallen.

Wenn TLS Zertifkate auslaufen und man hat kein gut funktionierendes Trackingverfahren im Einsatz, dann wird das TLS Zertifkat plötzlich aufhören zu funktionieren. Das Resultat kann für ein Unternehmen immense Auswirkungen haben, beispielsweise den Imageverlust eines Unternehmens, aber ein Grossteil dieser Unternehmen erleben auch einen finanziellen Verlust. Manchmal kann das einen Verlust von mehreren Millionen Euro pro Tag bedeuten, manchmal aber auch mehrere Millionen Euro pro Stunde. Leider kommt das nicht selten vor, Man hört von diesen Ausfällen von großen Unterenehmen immer wieder in den Medien, die müssen wir hier heute nicht nennen, aber die kommen öfter vor als es sein sollte.

11:10
Was koennen Unternehmen machen um diese Situation zu vermeiden?

Wenn ich die Frage richtig verstanden habe, was koennen Unternehmen dagegen unternehmen. Grundsätzlich könnten Unternehmen 3 Sachen dagegen vornehmen:

Eins: Unternehmen müssen TLS Zertifikate erstmals in deren Infrastrukturen finden. Zu unserer Überraschung gibt es sehr viele Unternehme die erstmal gar nicht wissen, wieviele TLS Zertifiakte sie wirklich besitzen oder wofür sie diese nutzen.

Zweitens: Wenn die Unternehmen all ihre TLS Zertifikate gefunden haben, muessen Sie diese auch managen.

Und Drittens: sie brauchen dann auch eine Art von Reporting Tool.

Um auf den ersten Punkt zurückzukommen: die Ergebnisse der Suche. Grundsätzlich gibt es hier verschiedene Arten und Weisen wie ein Unternehmen seine TLS Zertifikate finden kann. Sie können sich beispielsweise CT Logs (Certificate Transparency) Kollektoren anschauen. Diese Systeme gehen hinaus und suchen alle öffentlichen TLS Zertifkate, die man auf seine Domains ausgestellt hat. Desweiteren gibt es Tools, wie wir eines haben z.B. wo man diese in eine strukturierte Suchumgebung importieren kann um ihre TLS Zertifikate finden zu können. Dann gibt es auch sogenannte DiscoveryTools die interne Scans durchführen oder aber auch Tools, die auf ihrem Netzwerk installiert werden können um ihre Netzwerkumgebung zu scannen. Dieses kann entweder als ein Hosted Client genutzt werden oder als OnPrem Installation, um Zertifkate zu finden, um diese dann einzubringen. Das ist eine sehr effektive Methode. Dieses Konzept , um die TLS Zertifkate zu endecken / zu finden ist sehr wichtig.

Wenn Sie dann alle Ihre Zertifikate entdeckt haben, muss man anfangen, diese dann auch zu managen! Das würde ich wahrscheinlich in 2 getrennte Segmente teilen:

*Der erste ist das **Tracking**. Dafür gibt es IT Service Management Tools wie ServiceNow, wo wir als erster eine zertifizierte APP dafür haben. Das ist ein Ticketing Tool mit dem Sie Zertifikate in ihre Systeme verfolgen, die Nutzung klären und wer diese managt. Viele CA's haben auch diese native Tools. Viele Enterprises haben diese auf ihren Plattformen integriert. Auch wir haben ServiceNow dort integriert sind. Das wäre der Aspekt des Tracking.*

13:32
*Der andere Aspekt hier ist das **managing**. Manchmal wird es Zertifkatsnutzung genannt, manchmal Orchestrierung oder auch Bereitstellung. Das Management dieser Zertifkate versucht die dazugehoerigen privaten Schlüssel auf den dazugehörigen Endpunkten im Netzwerk bereitzustellen, wo sie mit den entsprechenden Zertifikaten versehen, installiert und konfiguriert warden müssen.*

Diese Tools reichen von den bekannten kommerziellen Services wie CLM (Certificate Lifecycle Management) von Venafi. Dann gibt es auch Native Tools die von einigen CA's angeboten warden. Auch wir haben eines, das Certificate Hub heist. Oder auch ein weiteres für unsere TLS Zertifkate, das ermoeglicht nicht nur unsere TLS Zertifkate zu managen, sondern auch Dritt Partei Zertifkate wie beispielsweise die MicroSoft CA Zertifkate.

Dann gibt es andere Tools die einem mit der Automatiersierung helfen. Ein Beispiel hierzu ist ein Tool das Ansible heißt. Ansible vereinfacht das Konfigurations-Management und unterstützt bei den verschiedensten Infrastrukturbeduerfnisse, die man haben kann. Das heisst mit Ansible kann man seine Zertifkate verteilen, dazu gibt es auch einen Freeware Code, auf den jeder zugreifen kann. Dieser funktioniert mit unserem Zertifkatemanagement aber auch für andere Zertifkate wie von Microsoft CA. Diese native Integrationen kann man einfach herunterladen und in seinen Netzwerkbeduerfnisse installieren. Diese sind sehr hilfreich, um Zertifkate in Netzwerken zu verteilen und zu managen.

*Dann der Dritte punkt den ich ansprach war das "**Reporting**". Es ist wirklich wichtig, ein gutes reporting system zu nutzen. Nicht nur um zu wissen was an Zertifikaten ausgestellt an Zertifkaten wurde, sondern auch was generell genutzt wird. Diese Services werden auch generell von Enterprise CA's angeboten, wo es offensichtlich ist das einige besser funktionieren als andere. Diese Tools / Services koennen einem auch helfen um die Zertifikate zusammenzufassen, sei es ein Tool wie Venafi oder auch Native Tools.*

All diese Dinge, also FIND, MANAGE und REPORT sind die Kernpunkte – the name of the game. Sie müssen die Zertifikate finden, bevor man sie managen oder auch reporten kann. Dies sind die Punkte die Ihnen helfen Ausfälle zu vermindern und vor allem punkte die alle Unternehmen vornehmen muessen.

16:33
Apple hat angekündigt, die Laufzeit von Zertifikaten auf etwa ein Jahr zu senken. Was bedeutet das für die Unternehmen?

16:47
Sicher, also ich wuerde sagen hier gibt es 2 Pro's und Cons zu dem CLM (Certificate Lifecycle Management) – nur um diese Frage etwas zu strukturieren..

Das erste, also das Pro ist: viele leute sind der Meinung, dass Zertifikate mit kurzer Lebensdauer besser sind. Je kürzer ein Zertikat lebt, desto größer ist die Sicherheit.

Das zweite Pro ist: wenn man meint, dass kurz lebende Zertifkate besser sind, dann unterstützt das eine Automatisierungsfunktion zum managen der Zertifikate, was der Anreiz waere um CLM (Certificate Lifecycle mangement) zu automatisieren, mit möglichen Tools die ich gerade eben angesprochen habe.

Die Con's hier, wären eine stärke manuelle Belastung, Arbeitsaufwand, sowie auch ein finanzieller Aufwand. Dieser Personal und Kostenaufwand ist meistens höher, als man es einschätzt und erwartet. Es könnte für Sie heißen, dass es länger dauert und mehr kostet.

Dann als weiteres Con, kommt die Frage, wie kurz ist die lebensdauer von Zertifkaten? Was wäre zu kurz? Wo wäre hier ein Kompromiss, da man seine Zertifikate und Services ja auch am Laufen halten möchte. Momentan befinden wir uns in eine Phase um herauszufinden und zu messen, was die optimale Lebenslaufzeit für ein Zertifkat waere oder auch sein soll.

Vor einigen Jahre befanden wir uns in einer grossen Veränderung, wo wir die Laufzeit von Zertifikaten von 3 auf 2 Jahren gesenkt haben. Das war sehr erfolgreich. Und nun will Apple es sogar auf ein Jahr verkürzen. In Zukunft könnte es also noch kürzer sein koennte und Unternehmen müssen das serstehen.

Das wären mehr oder weniger die Pro's und Con's. Aber um mit den Con's weiter zumachen: wenn ich darüber spreche, dass Unternehmen Kosten haben, um diese Zertifikate bereitzustellen und auszurollen, lass Sie uns einmal ein Beispiel durchspielen.

Ein Unternehmen mit global 2000 Mitarbeitern, das eventuell 2 Jahre bräuchte um so ein Szenario auszurollen. Mit einem Team von 10 Personen, die dann aber auch Software und Services bestellen muessen, die eventuell ein Budget von 2 Millionen pro Jahr haben. Wenn man für das 10 Personen Team Kosten von ca. 100.000 Euro pro Jahr ansetzt, sind wir dann konservativ geschätzt auf 2 Jahre bei 4 Millionen Euro Kosten fuer ein globales Unternehmen. Wenn wir das jetzt für 1000 globale Unternehmen multiplizieren, dann reden wir hier über einen Markt von 400 Millionen Euro, ah nein, 4 Billionen Euro im Bereich für globale Unternehmen, und das ist eine hoher Betrag - wenn man es so betrachtet - über einen Zeitraum von 2 Jahren.

Das sind wirklich hohe Ausgaben und es kostet Sie Ihre Zeit. Und da muss man sich selbst fragen, wie sehr wollen wir das tatsächlich selbst machen, wobei wir in diesem Beispiel nur sie Globalen 2000 Unternehmen genommen haben. Aber auch andere Unternehmen müssen ihre Lösungen ausrollen.

Logischerweise sind diese Zahlen nur über den daumen gepeilte Schätzungen, aber auch wenn man hier die Zahlen höher oder niedriger einschätzt, geht es hier immer noch um signifikante Investitionen für das Unternehmen, sowohl finanziell als auch personell.

Chris, bitte erzähle uns etwas über Vergangenheit, gegenwärtige Trends und mögliche Visionen!

21:13
Gerne. Also, als ich in dieser Industrie angefangen habe, drehte sich alles um die Authentisierung der Identitäten, die sich in den Zertifikaten befanden. Die Informationen mit denen sich die Unternehmen präsentierten. Das waren die ersten Zertifkatstypen, OV (organization validated).

Dann ueber die vergangene Jahre, speziell die letzten 8 Jahre, hat sich über die Verschlüsselung alles für den Online Verkehr gedreht. Zum größten Teil war die Industrie hier erfolgreich, mittlerweile sind 82 % aller Webseiten verschlüsselt. Das ist zwar in einige Regionen mehr als in anderen, aber grundsätzlich glaube ich das wir sagen können das wir erfolgreich waren.

Nun, persönlich glaube ich, das der kommende Trend wieder Richtung Identität zurückgeht. Das heist, es geht wieder um die Authentisierung der Unternehmensinformationen in den Zertifkaten, damit die Komsumenten sehen können welches Unternehmen welche Webpage anbietet. Es geht darum, ein hohes Vertrauen zu schaffen, damit die Nutzer sicher sind, das Sie sich auch wirklich mit der Organisation unterhalten, mit denen sie auch wirklich kommunizieren wollen.

Um hier ein paar Beweispunkte aufzuzeigen:

Erstens: GDPR, das ist ein Prinzip das persönliche Daten reguliert. Und in dieser Regulierung gibt es auch ein weiteres Prinzip zur Transparenz. Einige Regulatoren glauben, das es um Transparenz geht, um die Unternehmensinformation der Öffentlichkeit offenzulegen. Und ich glaube, das es beginnt ein RECHT für die Bürger zu werden, zu wissen, mit wem sie kommunizieren, Und das könnte auch der nächste Schritt zur Regulation innerhalb der EU werden.

Dann als nächstes haben wir auch seit einigen Jahren die EIDAS, die die elektronische ID Authentisierung und die Trust Services reguliert. Das ist eigentlich eine rechtliche Rahmenbedingung, wie Unternehmen untereinander kommunizieren müssen. Der Ersatz der manuellen Unterschriften durch digitale Unterschriften. Ein Teil dieser Regulierung ist, dass die dafür genutzten Zertifikate auf höchsten Niveau auf beiden seiten der Transaktion identifiziert werden muessen, um einen rechtlichen Status zu erzielen.

Diese Dinge, die wir sehen koennen, treiben immer wieder den Identitaets Schwerpunkt in den Mittelpunkt. Das Konzept Identität wächst langsam immer mehr, wo wir natuerlich auch andere Katalysten haben wie Betrug, die quartalmäßig immer mehr werden und es zeichnet sich nicht ab, , das es abnehmen wird. Dieses sehen wir auch in unserer aktuellen Situation, mit dem Fall von Covid 19 tauchen immer mehr Betrugsseiten auf. Auch hier wird die Identität in der Zukunft eine immer größere Rolle spielen.

27:03

Ich glaub das einzige was ich hinzufügen würde wäre, das Unternehmen einen Verantwortung haben ihren Kunden gegenüber. Sie sollten ihre Webseiten so sicher wie möglich machen, wo auch einfache Vorkehrungen gemacht werden können wie Nutzername und Kennwörter, wo eine verschiedene Reihe von Technologien heutzutage genutzt werden können.

Insbesonders wenn man sensible Informationen kommuniziert wie finanzielle- oder Gesundheitsinformationen, wäre es besser einen 2FA (2 Faktoren Authentisierungs) Prozess zu nutzen. Natürlich hilft es wenn man sein Unternehmen auf höchstem Niveau seinen Kunden gegenüber identifier. Versuchen Sie so viel Validierungsmechanismen wie möglich zu nutzen, wenn Sie ihre Unternehmens Identität ihren Endnutzern gegenüber veröffentlichen.

Hier helfen Ihnen die EV Zertifikate (extended validation), die eine großartige Möglichkeit ist, dieses zu erzielen. Sie sind immer noch sehr popular. Die meisten Banken nutzen diese heutzutage, wie DB, ING or JP Morgan Chase. Ich würde Ihnen raten, das zu machen und stellen Sie auch sicher, das Sie ihre Kunden darüber informieren, dass Sie diese Sicherheitsvorkehrungen implimentiert haben, um ihnen mehr sicherheit zu geben und nicht betrogen zu werden. Es ist oft überraschend zu sehen das man mit wenigen Informationen seine Kunden schlau machen kann, sie darüber informiert, wie sie profitieren und sich besser schützen können.

Am Ende sitzen wir alle im gleichen Boot, wir müssen eine gut geschützte Umgebung schaffen. Das würde ich vorschlagen und wir können für all unsere Kunden mit wenig viel erreichen.