STORMSHIELD

MEINUNGEN

CYBER-SICHERHEIT: EUROPA ALS HOCHBURG

Matthieu Bonenfant
Chief Marketing Officer,
Stormshield

Es gab einmal eine Zeit während des Kalten Krieges, als sich die Ost- und Westmächte ein Wettrennen um die Eroberung des Weltalls lieferten. Jetzt ist der Cyberraum das Ziel des Wettrennens. Die Herausforderungen für die Großmächte bleiben im Wesentlichen gleich, aber die Regeln haben sich geändert: Es gilt, seine Dominanz gegenüber dem Gegner zu festigen, indem man die neuen Spielfelder des digitalen Raums und die daraus resultierenden Fragen der Cyber-Sicherheit beherrscht bzw. meistert. Zu den teilnehmenden Teams gehören die USA, China, Russland oder auch Israel. Obwohl auch Europa involviert ist, scheint es aus der Ferne an diesem Rennen teilzunehmen. Wenn es um Angriffs- und Verteidigungsstrategien geht, setzt Europa vorzugsweise auf Werte wie Transparenz und Vertrauen. Hierdurch könnte es sich letztlich an die Spitze setzen. Die Werkzeuge hierzu besitzt es bereits.

GEOPOLITIK ALS ZENTRALES ELEMENT DER DIGITALTECHNIK

Es ist nicht mehr möglich, über Digitaltechnik und Telekommunikation zu sprechen, ohne politisch und geopolitisch zu denken. Schon seit einigen Jahren zeichnen sich unter dem Deckmantel der Cyber-Sicherheit die verschiedenen Angriffs- und Verteidigungsstrategien der Großmächte wie die Vereinigten Staaten, China, Russland und Israel ab.

Die mächtigsten digitalen Player scheinen sich mehr denn je staatlichen Weisungen bzw. Vorgaben unterordnen zu müssen: während die enge Zusammenarbeit zwischen NSA und amerikanischer Regierung gefestigt ist, wird ihrem russischen Pendant häufig vorgeworfen, die Hände bei raffinierten Cyber-Angriffen im Spiel zu haben. *„Was die chinesische Seite anbetrifft, so ist allgemein bekannt, dass es in der Nähe von Shanghai ein Gebäude gibt, in dem Offiziere der chinesischen Armee untergebracht sind, die als „Cyber-Krieger" ausgebildet wurden. Auf israelischer Seite wird das digitale Ökosystem größtenteils von ehemaligen Mitgliedern der Unit 8200, der Geheimdiensteinheit der israelischen Verteidigungsarmee getragen. Dies zeigt, welchen Platz heutzutage die defensiv wie offensiv agierenden „Cyber-Streitkräfte" auf der höchsten Ebene der strategischen nationalen Interessen einnehmen"*, erklärt **Pierre-Yves Hentzen**, Präsident von Stormshield. **Welchen Platz wird Europa bei diesen Machtspielen im Kampf um den Cyberraum einnehmen?**

Die Covid-19-Krise hat die Abhängigkeit Europas von diesen Großmächten bei Fragen der digitalen Souveränität verdeutlicht. Dennoch *„ist Souveränität nicht gleichbedeutend mit Abkapselung und Zurückgezogenheit, sondern steht tatsächlich für Freiheit: die Freiheit, Herr der eigenen Entscheidungen und Handlungen zu bleiben, ohne unter dem Joch eines Dritten zu stehen. Deshalb möchte ich gern sagen, dass Souveränität ein Thema ist, das nicht auf nationaler Ebene betrachtet werden darf. Ich höre oft, dass „unsere französischen Unternehmen geschützt und gefördert werden müssen", aber diese Aussage ist kontraproduktiv und stark vereinfachend. Es bedarf einer stärkeren globalen Bewegung für ein starkes, international anerkanntes Europa"*, betont Pierre-Yves Hentzen. *„Der Besitz von digitalen Infrastrukturen in Europa ist eine gute Sache, aber ihre Integrität und ihre Unabhängigkeit sind nicht gewährleistet, wenn zu ihrem Schutz im Hintergrund nicht-europäische Technologien zur Cyber-Sicherheit eingesetzt werden. Angesichts dieser geopolitischen Herausforderungen und des daraus resultierenden Misstrauens hatten bei der Auswahl eines Sicherheitsprodukts Kriterien die Produktherkunft betreffend eindeutig Vorrang vor rein technologischen Kriterien. Europa muss seine Haltung ändern und einer aktive Rolle übernehmen. Es verfügt über die nötigen Mittel - dies hat Europa bereits in anderen Bereichen im Kampf gegen die Gesundheitskrise und bei der Unterstützung der Industrie bewiesen - jetzt muss es auch im Bereich der Cyber-Sicherheit aktiv werden."*

DIE NOTWENDIGKEIT EINER FINANZIELLEN UND STAATLICHEN UNTERSTÜTZUNG

Durch die Covid-19-Krise offenbarte sich auch ein gewisser Rückstand Europas in Fragen der digitalen Souveränität. *„Wir waren nicht bereit. Am Beispiel der Videokonferenzlösungen sieht man, dass es amerikanische Firmen wie Zoom sind, die die Situation zu ihren Gunsten zu nutzen wissen und mit einem extremen Anstieg der Anzahl der Nutzer auf mehr als 200 Millionen pro Tag profitieren. Und das, obwohl es europäische Lösungen gibt, die jedoch, wie sich gezeigt hat, nur eingeschränkte Funktionen bieten, was manchmal auch auf Sicherheitsgründe zurückzuführen ist. Außerdem kämpfen sie aus Mangel an finanziellen Mitteln ums Überleben"*, betont Pierre-Yves Hentzen. Kosten für die Sicherheit, die als Nebeneffekt dazu führen können, dass die Investitionen in Funktionalitäten verringert werden. *„Was uns dazu bewegt, ein amerikanisches Produkt zu kaufen, das ist nicht nur eine Frage der Produktqualität, sondern auch die Tatsache, dass sie besser beworben, besser vermarktet werden"*, fügt Pierre-Yves Hentzen hinzu. *„Und dies ganz einfach, weil sie von finanziellen Unterstützungen profitieren, die dies ermöglichen."*

> *„Was uns dazu bewegt, ein amerikanisches Produkt zu kaufen, das ist nicht nur eine Frage der Produktqualität, sondern auch die Tatsache, dass sie besser beworben, besser vermarktet werden. Und dies ganz einfach, weil sie von finanziellen Unterstützungen profitieren, die dies ermöglichen."*
>
> **Pierre-Yves Hentzen,** Präsident von Stormshield

Dies scheint sich jedoch zu ändern: In Frankreich wurde beispielsweise angekündigt, dass rund zwanzig Investoren 6 Milliarden Euro zur Finanzierung der Start-ups der French Tech-Initiative bereitstellen werden. Es handelt sich nicht um öffentliche Gelder, sondern um Gelder aus den größten französischen Investmentfonds. Das Problem: in Europa scheint es leichter zu sein, in Technologien mit sofortiger Rendite zu investieren. Anwendungen, die erhebliche Investitionen in Forschung und Entwicklung erfordern, können allerdings nicht nach einem einzigen Jahr rentabel sein. Somit kommen die weltweit führenden Unternehmen, die sich solche Investitionen in die Cyber-Sicherheit leisten können, aus Amerika oder Israel. *„Die amerikanischen Unternehmen der Branche sind in der Regel an der Börse, der Nasdaq, notiert und werden vorteilhafterweise durch Private Equity Fonds finanziert, die es ihnen ermöglichen, jedes Jahr Hunderte Millionen Dollar in F&E und Marketing zu investieren, damit sie das Wachstum der Märkte für sich nutzen und die Märkte beherrschen können. Ihre Strategie besteht nicht im Streben nach sofortiger Rentabilität, sondern im Gewinn von Marktanteilen, der für ihre Bewertung maßgeblich ist. Und leider fördern unsere eigenen französischen Entscheidungsträger, ob es sich nun um private oder öffentliche Käufer handelt, diesen gut geölten Mechanismus, da sie hauptsächlich amerikanische Technologien erwerben"*, so Pierre-Yves Hentzen. Als Beispiel aus dem Gesundheitswesen in Frankreich nennt er den „Health Data Hub",

für den ursprünglich Microsoft mit dem Datenhosting beauftragt worden war. Diese Entscheidung löste aus gutem Grund einen Schrei der Empörung aus: Das französische Unternehmen OVHcloud investiert stark in diesem Bereich und hätte eine legitimere strategische Wahl für das Hosting derart sensibler Daten sein können. Ein Fall, der genau wie der von Photonis verfolgt werden muss: dieses Unternehmen, das sensible Hochtechnologien an Armeen liefert, wäre beinahe in amerikanische Hände gefallen. Das Ministerium für Wirtschaft und Finanzen hat bei diesem Verkauf sein Veto eingelegt. Das Unternehmen sucht immer noch nach französischen und europäischen Investoren, sollte es aber auf dieser Seite des Atlantiks keine akzeptable Lösung finden, könnte die USA wieder ins Spiel kommen ...

WIE WICHTIG ES IST, WIEDER DIE KONTROLLE ZU ÜBERNEHMEN

Finanzielle Unterstützung und Beherrschung von Infrastrukturen gehen Hand in Hand. China hat ein Internet, das von einheimischen Firewalls kontrolliert wird, um nicht vom Westen abhängig zu sein, insbesondere nicht von den Vereinigten Staaten. Russland folgte seinem Beispiel im letzten Jahr, indem es sein Internet von globalen Servern isolierte: ein Erfolg nach Meinung der russischen Regierung, die ein Gesetz zugunsten eines souveränen Internets vorschlagen will. „*Die eigentliche Herausforderung in diesem Zusammenhang bzw. Machtspiel besteht mittlerweile darin, die eigenen Infrastrukturen zu beherrschen, und dies schließt die Schutzmaßnahmen und -vorrichtungen mit ein. Die USA, China und Russland haben das verstanden. Israel hat vor einigen Monaten versuchsweise alle Zugänge zum Internet gesperrt, um zu sehen, ob das Land in der Lage ist, autonom zu funktionieren. Diese Fähigkeit, unabhängig funktionieren zu können, ist klar erkennbar*", erklärt Pierre-Yves Hentzen. Eine Ausgrenzung und Abkapselung, die die Frage nach Vertrauen aufwerfen.

Heute sehen wir jedoch, wie wichtig das Thema wird: Es wird deutlich, dass bestimmte Mächte nicht zögern würden, auf diese Mittel zurückzugreifen, um unsere Grundfeste ins Wanken zu bringen. **Europa kann hier seine Trümpfe mit seinen Werten der Offenheit und Transparenz ausspielen.** Während durch die DSGVO Einzelpersonen und ihre individuellen Rechte geschützt werden sollen, erlaubt der *Cloud Act* der USA den Zugriff auf die Daten aller Personen, sogar außerhalb der Vereinigten Staaten. Zwischen diesem sehr intrusiven System und dem Chinas, das sich mehr und mehr abkapselt und isoliert, steht Europa für Offenheit und Vertrauenswürdigkeit – und dies sogar noch mehr, nachdem der Europäische Gerichtshof den *Privacy Shield* (Datenschutzschild) für ungültig erklärt hat.

EIN EUROPÄISCHER RECHTSRAHMEN, DER EINER VEREINHEITLICHUNG BEDARF

Während sich die DSGVO als internationaler Maßstab etabliert, scheint der übrige europäischen Rechtsrahmen weniger einheitlich zu sein. Auf diesem internationalen Schachbrett scheinen drei europäische Länder bzw. Kräfte besser aufgestellt zu sein, hauptsächlich dank ihrer Sicherheitsbehörde. Frankreich mit der französischen Agentur für die Sicherheit von Informationssystemen (ANSSI), Deutschland mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und - in einer weiter gefassten Definition von Europa - das Vereinigte Königreich mit dem Nationalen Zentrum für Cyber-Sicherheit (NCSC) sind alle drei weltweit für ihren restriktiven Ansatz in Bezug auf die Sicherheit und den Schutz von Informationssystemen anerkannt und akkreditiert. Trotzdem bleibt festzustellen, dass Europa ein fragmentierter Markt mit unterschiedlichen Sprachen und Kulturen und ein nationaler Ankerplatz ist, der in den verschiedenen Mitgliedstaaten immer noch sehr präsent ist. Dies ist der Grund, warum ein Auftrag zur Cyber-Sicherheit in der Regel vorwiegend an ein Unternehmen im Wohnsitzland vergeben wird.

Ein Verlassen dieser Komfortzone bedeutet, dass Anstrengungen und Investitionen erhöht werden müssen. So müssen zum Beispiel Übersetzungen angefertigt, auf bisher unbekannte Medien zugegriffen und das Produkt oder die Dienstleistung an die verschiedenen Länder angepasst werden: Anstrengungen und Investitionen, die sich heute nur die Big Player leisten können. Eine Fragmentierung, die die Europäische Kommission insbesondere bei Anwendung der NIS-Richtlinie zur Netz- und Informationssicherheit fürchtet. Denn auch wenn diese bei der Einführung von Betreibern kritischer Dienste (OSE) *„in vielen Mitgliedsstaaten als Katalysator diente und dort den Weg für eine wirkliche Veränderung des institutionellen und rechtlichen Rahmens für die Cyber-Sicherheit ebnete"*, heißt es in einem jüngeren Bericht dass, *„sich die Auslegungen der Länder hinsichtlich der Art eines kritischen Dienstes unterscheiden. Es wird daher schwierig, die Listen der kritischen Dienste zu vergleichen."* Um dieser Fragmentierung entgegenzuwirken, ist eine Harmonisierung der Vorschriften unabdingbar: der Europäischen Agentur für Netzwerk- und Informationssicherheit, kurz ENISA, kommt somit eine wichtige Rolle beim Aufbau eines sicheren digitalen Binnenmarkes zu, der dem Binnenmarkt für Waren und Menschen auf digitaler Ebene entspricht.

In diesem Sinne und im Rahmen des Cybersicherheitsgesetzes sollen europäische Zertifizierungssysteme entwickelt werden, um den Markt zu vereinheitlichen. Der erste Entwurf eines Zertifizierungsschemas für Produkte zur Cyber-Sicherheit wurde gerade vorgestellt und basiert auf den bereits bestehenden Rahmenbedingungen. Dieser Entwurf wurde von der ENISA erstellt, die sich auf das Fachwissen der Mitgliedstaaten und Interessengruppen stützte, darunter auch Stormshield. *„Ziel ist es, diese Fragmentierung zu verringern und zu verhindern, dass ein Unternehmen für seine Produkte eine Zertifizierung in Anspruch nimmt, die in dem Land anerkannt und gültig ist, in dem es zum Beispiel seine Firewall vermarkten möchte; ferner soll verhindert*

werden, dass es immer mehr nationale Standards gibt“, bestätigt Philippe Blot, Lead Expert Certification der ENISA. „*Auf diese Weise sollen europäische Wege geschaffen und ein europäisches Regieren ermöglicht werden, wobei die entsprechenden Spielregeln von allen beteiligten Akteuren vereinbart werden. Die Zertifizierung ist eine wesentliche Voraussetzung für Vertrauen. Dies bedeutet, dass das Produkt eine Art „Feuerprobe“ bei einem Dritten bestehen muss. Bei diesem muss es sich um eine akkreditierte Stelle handeln, die unabhängig vom Anbieter ist und die von den im Rahmen des Systems eingerichteten nationalen Behörden beaufsichtigt wird. Durch dieses größere Vertrauen können die Angebote transparenter gestaltet werden. Darüber hinaus wird es den Markt für 500 Millionen Menschen öffnen*.“

„Auf diese Weise sollen europäische Wege geschaffen und ein europäisches Regieren ermöglicht werden, wobei die entsprechenden Spielregeln von allen beteiligten Akteuren vereinbart werden.“

Philippe Blot, Lead Expert Certification der ENISA

Nächster Schritt: die Cloud. Die ENISA wurde von der Europäischen Kommission mit der Ausarbeitung eines europäischen Zertifizierungssystems für die Cyber-Sicherheit von Cloud-Diensten beauftragt. Ein Projekt, das an Gaia-X erinnert, die europäische Cloud-Plattform, deren Ziel der Aufbau einer zuverlässigen und sicheren Dateninfrastruktur für Europa, insbesondere im Gesundheitsbereich, ist. „*Die eingesetzten Technologien zur Verschlüsselung müssen vertrauenswürdig sein und die entsprechenden Schlüssel müssen von dem Unternehmen selbst oder einem vertrauenswürdigen Partner aufbewahrt werden. Wo immer sie aufbewahrt werden, muss ich in der Lage sein, meine Daten wiederherzustellen: Dieser Begriff der Reversibilität ist von wesentlicher Bedeutung und Europa muss in diesem Sinn agieren*“, erklärt Pierre-Yves Hentzen.

EIN EUROPA, DAS EIN WENIG ZU BESCHEIDEN IST

Aber ist Europa nicht ein wenig zu bescheiden? *„Die USA, Asien und Israel haben eine starke Kultur des Unternehmertums entwickelt: Die Gründung eines Start-ups wird dort als echte Karrierechance angesehen. Die Regierungen unterstützen sie, ermutigen sie zu diesem Schritt und die Vorschriften sind dort flexibler als in Europa. Digital Champions werden eher dort geboren*", bekräftigt **Markus Braendle**, Head of Airbus CyberSecurity.

Europa muss sich jedoch nicht verstecken. Es beherbergt sehr kompetente Cybersicherheitsunternehmen und erstklassige Universitäten für die Forschung im Bereich der Cyber-Sicherheit mit hochtalentierten Cyber-Ingenieuren. *„Ich denke, wir sind zu bescheiden und schätzen unsere traditionellen Fähigkeiten nicht hoch genug ein. Mit Industrie 4.0 befinden wir uns mitten in einer neuen industriellen Revolution mit Branchenführern in der Luft- und Raumfahrt, der Automobilindustrie, der Pharmakologie und der Chemie, um die uns viele beneiden. Wir besitzen ein beispielloses Know-how, ein einzigartiges Wissen und hiermit sind noch größere Cyber-Gefahren verbunden. In diesem Sinne muss sich Europa die Frage stellen, inwieweit es beim Thema Cyber-Sicherheit von anderen abhängig sein möchte und wie die richtige Balance gefunden werden kann*", so Markus Braendle abschließend.

STORMSHIELD

Weltweit müssen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und erlauben den Schutz der Geschäftstätigkeit. Unsere Mission: Cybersorglosigkeit für unsere Kunden, damit diese sich auf ihre Kerntätigkeiten konzentrieren können, die für das reibungslose Funktionieren von Institutionen, Wirtschaft und Dienstleistungen für die Bevölkerung so wichtig sind. Die Entscheidung für Stormshield ist eine Entscheidung für eine vertrauenswürdige Cybersicherheit in Europa. Weitere Informationen finden Sie unter www.stormshield.com.