Kurier, 15.03.2018, Seite D4

Server, Hosting und die Cloud

Speicher. Die DSGVO lässt Unternehmen neu überlegen, wo sie ihre Daten sicher speichern

Anexia-CEO Alexander Windbichler wehrt für seine Kunden jede Stunde tausende Angriffe ab

Das österreichische Unternehmen Anexia wurde 2006 von CEO Alexander Windbichler in Klagenfurt gegründet, ist seit dem international gewachsen und konnte Anfang März 2018 die bisher größte Computerattacke in Österreich abwehren. Vereitelt werden konnte der Angriff durch die kürzlich fertiggestellte Infrastruktur „Backbone Europe". Anbieter wie Anexia stellen nicht nur sicher, dass die Services ihrer Kunden ohne Ausfall erreichbar sind, sondern auch, dass sensible Daten nicht in die falschen Hände geraten. Etwas, das mit der neuen DSGVO noch relevanter wird. Anexia ist ein Anbieter von Software, unterstützt seine Kunden bei der Digitalisierung und bietet Hybrid-Services an – maßgeschneiderte Modelle zwischen Serverhosting und Cloudservice. Zu den bekanntesten Kunden zählen etwa Netflix, die ihre Serien und Inhalte hier hosten, andere Kunden wählen Anexia wegen der gewünschten Diskretion und wollen nicht genannt werden. Vertrauen ist in der Branche entscheidend: „Kunden vertrauen uns ihre Daten an und es ist gar nicht allen bewusst, wie heikel das sein kann. Sie legen viel Wert auf Verlässlichkeit und Stabilität," erzählt Alexander Windbichler aus der Praxis. Dies beinhaltet auch eine sinnvolle Vision und Balance zwischen Innovation und dem Bemühen, Kunden vor ständigen Änderungen zu bewahren und nicht permanent neue Produkte einzuführen.

Gefahr: Erpresser

Bei Angriffen auf die Daten und Services von Unternehmen unterscheidet Windbichler zwei verschiedene Arten: „DDoS-Angriffe, wie jener Anfang März nehmen aktuell rasant zu. Diese DDoS-Attacken sind vergleichbar mit einer Lawine aus Daten. Hacker versuchen durch unzählige Anfragen aus einer Vielzahl unterschiedlicher Quellen, Server in die Knie zu zwingen und damit die dort laufenden Services lahmzulegen. Ziel solcher Angriffe sind Online-Portale, E-Commerce-Anwendungen oder Server mit hochsensiblen Daten. Insgesamt haben wir aktuell über 5000 Attacken pro Stunde auf unseren Servern und wissen auch von anderen Betreibern, die eine Steigerung an Angriffen registrieren." Er beschreibt das in einem anderen Bild wie einen Laden, in dem man etwas kaufen möchte, dessen Eingang aber von tausenden anderen Personen verstellt ist – Services werden dadurch unbrauchbar.

Eine andere Art von Angriff ist jener, dem etwa die Deutsche Bundesregierung derzeit ausgesetzt ist. Hier geht es konkret, um das Entdecken von Sicherheitslücken und den Diebstahl von Informationen: „Das hat schon etwas von Spionage," beschreibt Windbichler den Vorgang. „Zum einen ist Unternehmen oft jahrelang nicht bewusst, dass Fremde in ihrem System sind und zum anderen werden genau diese Angriffe nun auch im Rahmen der DSGVO relevant." Unternehmen sind hier haftbar und im Fall eines Problems, gibt es eine Meldepflicht. Da die vorgesehenen Strafen in Zukunft außerdem sehr hoch sind, rechnet Windbichler in diesem Bereich mit neuen Verbrechen und Erpressungen: „Manche Unternehmen werden, bevor sie Datenlecks zugeben und melden und eventuell mit hohen Strafen rechnen müssen, überlegen Erpresser zu bezahlen."

Hybridlösungen

Es gilt für Unternehmen noch mehr als zuvor zu überlegen, welche Speicherlösungen für sie die besten sind. Dazu können physische Server im Büro zählen, angemietete Server bei einem Dienstleister oder auch Cloudservices, die auch in Mischformen miteinander verbunden werden können. Die Lösungen müssen individuell sein: „Während es am Land teilweise immer noch schwer ist, sich über entsprechende Datenleitungen mit Servern und Clouddiensten zu verbinden, haben viele Büros auf der anderen Seite keine für Server geeigneten Räume oder auch entsprechenden Brandschutz," weiß Windbichler. Entscheidend ist für Kunden deswegen nicht nur der Preis, sondern auch die richtige Beratung und Flexibilität: „Es ist für Kunden ein Problem, wenn sie sich von einem Anbieter oder Produkt abhängig machen sollen. Teilweise geht es hier auch darum, dass mehrere Anbieter – gemeinsam statt gegeneinander – die richtige Strategie für einen Kunden finden." Für österreichische und europäische Anbieter ist die kommende DSGVO ein großer Nachfrage-Treiber.

„Kunden vertrauen uns ihre Daten an und es ist gar nicht allen bewusst, wie heikel das sein kann. Sie legen Wert auf Verlässlichkeit und Stabilität."

Alexander Windbichler, Anexia

Standort Europa

Schon bisher ist etwa die sich immer wieder ändernde Regelung von Interesse, ob amerikanische Cloudanbieter ihrer Regierung auf Anfrage die Daten ihrer Kunden aushändigen müssen.

„Diese Unsicherheit macht es für Unternehmen in Europa – und eigentlich überall außerhalb von Nordamerika – interessant, sich nach europäischen Dienstleistern und Angeboten umzusehen." Noch wichtiger wird dies im Zusammenspiel mit der DSGVO, nachdem Unternehmen hier Datenleaks auf jeden Fall verhindern wollen und die Gewährleistung und Haftung nicht an externe Anbieter weitergeben können.

Anexia und andere österreichische und europäische Anbieter punkten hier aktuell nicht nur mit dem Standort, sondern auch der entsprechenden Beratungsleistung, die auch beinhaltet, dass man Kunden Formulare und Vorlagen zur Verfügung stellt.

– MARTIN MÜHL

Mit einer Infrastruktur wie hier dem Projekt Backbone Europe rüsten sich Anbieter gegen Online-Angriffe, DDoS-Attacken und Datendiebstahl