HWZ
Die Hochschule für Wirtschaft
in Zürich

Cyber Security Trends 2019 – Was neu auf den Radar muss

VON RALPH HUTTER, Studiengangsleiter CAS Cybersecurity, Compliance & RegTech an der HWZ Hochschule für Wirtschaft Zürich

Zürich, April 2019

Das Internet ist 30 Jahre alt. Ein Grossteil der Weltbevölkerung hat Zugang zum World Wide Web. Online Commerce ist etabliert, Plattform-Geschäftsmodelle dominieren zahlreiche Branchen und mobiler Zugang hat den Desktop schon lange überholt. Man würde meinen, dass Informationssicherheit bzw. Cyber Security längst etablierte Themen seien. Weit gefehlt.

Die rasante Verbreitung von IoT-Geräten, neuen Plattform-Geschäftsmodellen auf Cloud Basis – API Zugang inklusive – verursachen eine Vervielfachung der Angriffsflächen für Cyberkriminalität. Die zunehmenden Medienberichte über Databreaches auch bei grundsätzlich vertrauenswürdigen Firmen und die Publizität um die Einführung der europäischen Datenschutz-Grundverordnung DSGVO führen zu mehr Sensibilität bezüglich Schutz der Privatsphäre bei Konsumenten. Eine Übersicht über die wichtigsten Trends und Herausforderungen im Bereich Cyber Security für 2019, die auf die Agenda im Management gehören.

Cloud-Sicherheit ist nicht nur Providersache

Viele Unternehmen haben kritische Anwendungen, Prozesse und Daten auf Cloud-Plattformen grosser Anbieter wie Amazon Web Services (AWS) oder Microsoft Azure verschoben, in der Meinung, sie hätten damit alle Sicherheitsfragen delegiert. Im Jahr 2018 gab es mehrere drastische Vorfälle in Public-Cloud-Umgebungen. Allerdings ist die Mehrheit der Verstösse nicht auf Fahrlässigkeit der Cloud-Service-Provider zurückzuführen, sondern auf mangelnde Governance auf der Kundenseite. Während Cloud Service Provider für den Schutz der Infrastruktur verantwortlich sind, bleiben die Cloud-Kunden in der Pflicht, die Governance der Zugangsberechtigungen, die Einhaltung der Compliance sicherzustellen und auch kritische Prozesse, anormale Benutzeraktivitäten und verdächtigen Netzwerkverkehr zu überwachen. Darüber hinweg muss sichergestellt sein, dass im Rahmen der immer populärer werdenden containerisierten Anwendungen auch substanzielles Security Know-how über den gesamten Entwicklungs- und Releaseprozess vorhanden ist.

Zero-Trust Architektur – Ein neues Denkmodell muss her

Cloud-Anwendungen boomen, aber die meisten Netzwerkarchitekturen sind schon ziemlich in die Jahre gekommen und setzen noch auf altbewährte Zonenkonzepte, die sich auf den Schutz des Perimeters fokussieren. Wenn ein Angreifer diesen Perimeter überwunden hat, kann er sich im Netzwerk bewegen oder wenn neue Anwendungen z. B. in der Cloud betrieben werden, greift der Perimeterschutz nicht mehr. Abhilfe schafft eine Zero-Trust-Architektur. Das Modell wurde bereits 2010 von John Kindervag entwickelt, der damals Analyst bei Forrester Research war. Angesicht der zahlreichen Databreaches ist es heute aber aktueller denn je.

Das Zero Trust Sicherheitskonzept basiert auf der Idee, dass Unternehmen etwas nicht automatisch innerhalb oder ausserhalb ihrer Netzwerkgrenzen vertrauen sollten, sondern stattdessen alle Verbindungen individuell im Kontext von Mikrosegmentierung bzw. Mikroperimeter beurteilen und berechtigen müssen. Noch einfacher gesagt: Zero Trust – Vertraue grundsätzlich niemandem.

Conversational Interfaces für Authentifizierung
Conversational Interfaces sind in erster Linie durch die Personal Assistants Siri von Apple, Alexa von Amazon, Cortana von Microsoft oder Google Assistant bekannt. Unter dem Begriff werden auch Chatbot-Anwendungen für text- oder sprachbasierte Anwendungen im Kundendienst subsummiert. Neu am Markt sind nun auch Dienste, die Spracherkennung zur Authentifizierung im Call Center wie beispielsweise bei Swisscom verwenden. Dazu wird ein Sprachabdruck des Kunden aufgezeichnet, der bei künftigen Anrufen die Identifikation übernimmt und damit lästige Sicherheitsfragen erübrigt. Die USAA Banking App geht noch einen Schritt weiter und kombiniert die Spracherkennung mit weiteren biometrischen Merkmalen wie Fingerabdruck und Gesichtserkennung zur Erhöhung der Sicherheit bei der Authentifizierung. Kritisch zu betrachten sind dabei die transparente Kommunikation bei der Einführung, ein datenschutzkonformes Onboarding und vor allem die Datensicherheit der biometrischen Daten der Kunden.

Privatsphäre wird zum Geschäftsmodell
Die Einführung der Datenschutz-Grundverordnung der EU (DSGVO) im Mai 2018 wird zum Wendepunkt im Datenschutz. Erste verhängte Geldbussen bei Verstössen und die langsam anlaufende Strafverfolgung zeigen, dass die DSGVO den Datenschutz nicht nur in der EU sondern auch die international massgeblich beeinflusst. Privacy by Design und eine internationale Kompatibilität wird notwendig, um sich vor Klagen zu schützen oder aber auch um sich mit dem Thema Datenschutz zu positionieren oder gar ein Geschäftsmodell daraus zu machen.

Am Beispiel Apple: Bei der letzten Keynote von Apple unterstrich Tim Cook, warum sich die Apple-Dienste differenzieren: «Sie sind so konzipiert, dass Ihre persönlichen Daten vertraulich und sicher bleiben», sagte er dem Publikum. Insbesondere auch im Hinblick auf neue Produkte wie ein neuer Newsdienst oder eine Kreditkarte. Gleichzeitig kämpft Facebook gegen den Vertrauensverlust nach zahlreichen Datenpannen. Mark Zuckerberg hat in einem langen Artikel «A Privacy-Focused Vision for Social Networking» die neue Ausrichtung von Facebook von öffentlicher Kommunikation hin zu privaten Interaktionen als Grundlage für neue Produkte angekündigt.

Privatsphäre, Sicherheit und Konformität zu Datenschutz werden die Grundlagen für eine vertrauensvolle Kundenbeziehung und die Reputation eines jeden Unternehmens sein.

API Security by Design
Wir leben in der Ära der API-Ökonomie. In den letzten zehn Jahren ist die Anzahl verfügbarer Programmierschnittstellen exponentiell gewachsen. ProgrammableWeb.com verfügt über ein Verzeichnis mit über 21’000 APIs. Diese ermöglichen z. B. Online-Shops, Bezahldienstleister, Online-Marktplätze, Vergleichsplattformen und zunehmend IoT-Geräte durch einzelne Services einfach und schnell miteinander zu einem digitalen Ökosystem zu verbinden. Aber auch Legacy-Anwendungen werden umgerüstet. Unternehmen zerlegen

ihre Software in kleinere Teile, um diese über APIs für interne oder externe Frontendanwendungen zugänglich zu machen.

Mit der Verbreitung von APIs steigt jedoch auch das Potenzial für weitere Sicherheitslücken. Systeme, Daten und Anwendungen werden neu einfacher und standardisiert verfügbar gemacht. Damit diese nicht versehentlich zugänglich gemacht werden, muss ein ganzheitliches Konzept für API-Security-Architektur bereits vor der Entwicklung einzelner API erarbeitet werden. Dazu gehören Einsatz von Verschlüsselung, Fokus auf Authentisierung und Autorisierung, Monitoring, regelmässiges Vulnerability Testing. Ein Anknüpfungspunkt ist z. B. das OWASP API Security Project des OWASP-Konsortiums, das sich auf die Verbesserung der Softwaresicherheit konzentriert und die häufigsten API-Schwachstellen überwacht.

Cyber Security Awareness – Sensibilisierung der Benutzer ist Daueraufgabe
Das schwächste Glied in der Sicherheitskette ist nach wie vor der Mensch. In der Kill Chain eines Cyberangriffs werden für die Aufklärung und Vorbereitung hauptsächlich Social Engineering- und Phishing-Techniken angewandt, die sich gegen Anwender bzw. Mitarbeitende wendet. Die Statistik von Fedpol für 2018 zeigt auf, dass es bei 19 % der gemeldeten Cybercrime Vorfälle in der Schweiz um Phishing-Angriffe handelt. Dunkelziffer unbekannt.

Dazu gesellt sich mangelndes Bewusstsein bei Mitarbeitenden. Dieses äussert sich in der Verwendung von Arbeitsplatzgeräten für persönliche Transaktionen, im Herunterladen nicht genehmigter Software, Schatten-IT wie privat genutzte Anwendungen, z. B. Clouddienste oder Kommunikationstools wie Instant Messaging, oder eben durch die Aktivierung bösartiger Anhänge in E-Mails. Ein regelmässiges Security Awareness Training erhöht das Verantwortungsbewusstsein und hilft, eine Kultur des Vertrauens zu schaffen, in welcher mögliche Incidents nicht verschwiegen, sondern aktiv durch Mitarbeiter informiert werden.

Quellen

https://www.faz.net/aktuell/technik-motor/digital/30-jahre-world-wide-web-das-internet-feiert-geburtstag-16078501.html

https://www.forbes.com/sites/forbestechcouncil/2019/02/07/five-cybersecurity-trends-to-watch-for-in-2019/#f9747af4c66a

https://www.techrepublic.com/article/5-cloud-security-trends-to-watch-in-2019/

https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

https://go.forrester.com/blogs/next-generation-access-and-zero-trust/

https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/ch01.html

https://www.united-security-providers.ch/blog/zero-trust-architekturen-vertrauen-ist-gut-kontrolle-ist-besser/

https://thefinancialbrand.com/66697/usaa-conversational-ai-voice-chatbot/

https://findbiometrics.com/solutions/voice-speech-recognition/

https://techbeacon.com/app-dev-testing/8-essential-best-practices-api-security

Der Zertifizierungslehrgang zum Thema

CAS Cybersecurity, Compliance & RegTech: www.fh-hwz.ch/casccr

HWZ Hochschule für Wirtschaft Zürich
Lagerstrasse 5, Postfach, 8021 Zürich
043 322 26 88, master@fh-hwz.ch, www.fh-hwz.ch