Foto: IBM Market Asset Manager

Robert Kernstock

Umfassender Schutz unternehmenskritischer Daten

Vorneweg ein möglicherweise entmutigendes Statement: niemand kann sich vor Cybercrime-Attacken schützen. Know-How und technische Möglichkeiten von Cyberkriminellen sind auf höchstem Niveau, und wie in anderen kriminellen Bereichen auch sind die „Guten" immer einen Schritt hinter dem „Bösen" zurück. Man kann sich eine Botnet-Ausstattung bereits um wenige 100 Euro online im Internet kaufen, und mit Hilfe der hervorragenden Dokumentation auch ohne besondere Kenntnisse damit gezielte Angriffe starten. Nach oben ist die Grenze naturgemäß offen, ebenso wenig das Ausmaß der Schäden.

Unser Wirtschafts- und Sozialleben ist angewiesen auf elektronische Kommunikation: beispielsweise würde eine Bank deren elektronisches Kommunikationssystem durch einen gezielten Angriff lahmgelegt wird, nach etwa drei Tagen in massive wirtschaftliche Schwierigkeiten geraten. Vergleicht man die sicherheitstechnischen Grundlagen der Kommunikationssysteme mit anderen Bereichen kritischer Infrastruktur, beispielsweise dem Straßenverkehr, so fällt auf dass im Verkehrsbereich eine Vielzahl von gesetzlichen und technischen Rahmenbedingungen sowie Know-How der Verkehrsteilnehmer existieren die es dem Benutzer ermöglichen relativ sicher von A nach B zu kommen. Dies ist bei elektronischen Kommunikationssystemen großteils nicht der Fall: es fehlen in weiten Bereichen Grundlagen bzw. beruhen diese auf Standards die keine rechtliche Verbindlichkeit haben, beispielsweise bei Identifikations- und Autorisierungsverfahren. Wäre es möglich ein KFZ mit unterschiedlichen Kennzeichen zu versehen und mehrere Führerscheine zu besitzen, oder das KFZ je nach Lust und Laune mit verschiedenen Kraftstoffen zu betreiben? Während man einem KFZ-Halter zumindest ein Basiswissen über Airbags, Gurtsysteme, Winterreifenpflicht etc. zubilligen kann, darf man aber bezweifeln dass der durchschnittliche Internet-Benutzer das Thema Virenschutz, Passwortregeln und Identitymanagement wirklich anwendet. Man kann auch davon ausgehen dass der Straßenerhalter rechtzeitig vor Gefahren wie Glatteis, Lawinen oder Staus warnt, während dies beim Internet in erster Linie auf Eigeninitiative beruht.

In diesem Umfeld stellt ein umfassender Schutz vor Cyber-Bedrohungen für Unternehmen eine Herausforderung dar. Man muss sich allerdings fragen was wirklich eine Bedrohung für ein spezifisches Unternehmen darstellt. Nach übereinstimmender Expertenmeinung sind dies sog. Advanced Persistant Threats, also langandauernde technisch gefinkelte und vor allem gezielte Angriffe die den Zugang zu sensiblen Daten zum Ziel haben. Sensible oder unternehmenskritische Daten sind jene Informationen, die das Überleben einer Organisation sichern, beispielsweise Vorstandsinformationen, Übernahme- und Verkaufspläne, geistiges Eigentum, Kundeninformationen, etc. Sie machen nur wenige Prozent des gesamten Datenbestandes aus, stehen aber für etwa 70 Prozent des Unternehmenswerts. Sie haben größten Einfluss auf Wachstum, Reputation und Markenwert. Trotz des enormen Stellenwerts dieser sensiblen Daten verfahren viele Unternehmen damit leichtfertig, wissen beispielsweise nichts über Lage, Zugangsberechtigungen und Schutz dieser Daten. Das macht die Überwachung und ihren Schutz sehr schwie-

rig. Tatsächlich braucht es in über 95 Prozent der Fälle oft Tage oder mehr, bis ein Datenverlust bemerkt wird. Zudem sind in 90 Prozent der Fälle Wochen oder Monate notwendig, um Sicherheitslücken zu schließen, von denen potenziell massive Gefahren für das Geschäft ausgehen.

Der IBM X-Force-Threat Intelligence Report basiert auf Auswertungen von nahezu 1.000 Kundensituationen in 133 Ländern und liefert dazu recht eindrucksvolle Daten: Im ersten Halbjahr 2014 wurden z.B. zwölf Prozent mehr Sicherheitsvorfälle als im Jahr zuvor entdeckt – das sind 91 Millionen Vorfälle insgesamt oder durchschnittlich 1,7 Millionen pro Woche. Der Anstieg von Spam erreichte dabei den höchsten Wert in den vergangenen 2,5 Jahren, womit E-Mails als Mittel für die Verbreitung von Malware unangefochten an erster Stelle bleiben. Allerdings schließt ein Großteil der Attacken in irgendeiner Weise menschliches Fehlverhalten mit ein – entweder weil ein Mitarbeiter zum Beispiel durch Doppelklick einen infizierten Anhang oder eine URL geöffnet hat, einen Default-Nutzernamen und Passwort genutzt oder vertrauliche Informationen an falsche Adressaten geschickt hat:

Eine sinnvolle Abwehr von Cyberattacken kann mit einem permanenten Monitoring realisiert werden:

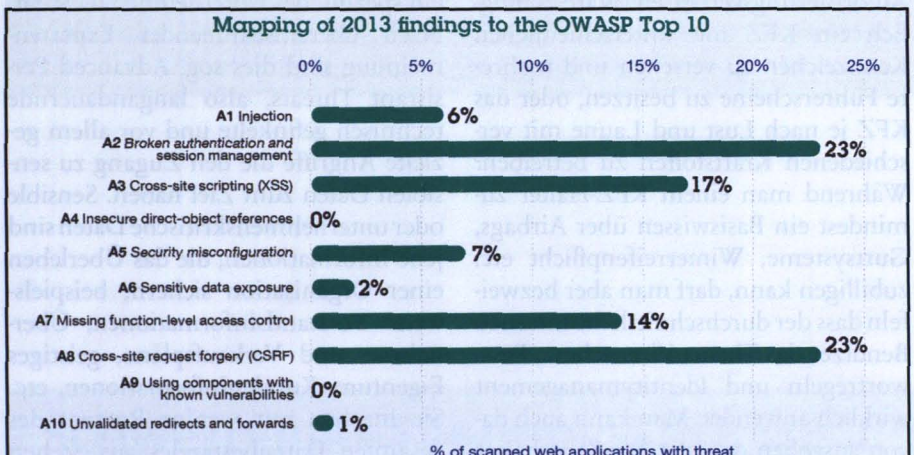

Figure 1. Common vulnerabilities found occurring in web applications tested by the IBM Hosted Application Security Management (HASM) service, compared to the OWASP Top 10 for 2013

Quelle: X-Force Threat Intelligence Quarterly 2014

- Wer greift an?
- Was ist das Ziel der Attacke?
- Wie wird die Attacke technisch durchgeführt?
- Stellt die Attacke eine Bedrohung dar?

Anstatt zu versuchen das eigene Netzwerk zu 100 % abzusichern (was technisch und finanziell extrem aufwendig ist und in Wahrheit nie realisiert werden kann) begegnet man den Angreifern mit Intelligenz, indem die Attacken in „Real Time" analysiert und das Bedrohungspotential bewertet wird. Wenn eine bedrohliche Attacke erfolgt, ist man durch die Information über die Attacke sofort in der Lage entsprechende Maßnahmen einzuleiten. Dies setzt natürlich voraus dass man diese Attacken kennt. X-Force erforscht permanent die weltweit durchgeführten Attacken und liefert die Angriffsvektoren an eine Datenbank, welche eine wesentliche Informationsquelle für Security Information und Event Management Systeme (SIEM) darstellt.

Üblicherweise besteht die IT-Security meist aus einzelnen, nicht miteinander kommunizierenden Komponenten, organisatorisch sowie technisch. Der Einsatz einer integrierten SIEM-Lösung stellt sicher dass die Informationen aus allen Security-Komponenten auf einer zentralen Informationskonsole verarbeitet werden und mit voreingestellten Sicherheitsregeln permanent abgeglichen werden. Damit werden auch Fälle aufgedeckt wie jener aus einer konkreten Kundensituation, der mit konventionellen Securitykomponenten unentdeckt bleibt: ein Mitarbeiter loggt sich zu einer Zeit am Unternehmensstandort ein den er laut Zutrittssystem gar nicht betreten hat, legt einen Benutzer mit umfassenden Zugriffsrechten an, loggt sich mit diesem erneut ein, führt eine Datenbankabfrage auf Kundendaten durch, speichert die Daten auf einem Datenträger der auf der fraglichen Workstation eigentlich nicht zulässig ist, und löscht den Benutzer anschließend wieder ... ein korrekt konfiguriertes SIEM-System produziert sofort einen Alarm und speichert den Vorfall sodass der gesamte Angriff nachvollziehbar und transparent wird.

Eine besondere Problematik ergibt sich im Bereich der Fertigungsindustrie. Das Schlagwort Industrie 4.0 ist in aller Munde: Ziel ist die intelligente Fabrik (Smart Factory), die sich durch Wandlungsfähigkeit, Ressourceneffizienz und Ergonomie sowie die Integration von Kunden und Geschäftspartnern in Geschäfts- und Wertschöpfungsprozesse auszeichnet. Technologische Grundlage sind Cyberphysische Systeme und das Internet der Dinge (Quelle: Wikipedia).

Aus Sicht der IT-Security stellt dieses Konzept einen nicht zu vernachlässigenden Unsicherheitsfaktor dar. Experten sehen die Fertigungsindustrie als prädestiniert für Attacken an, da die Vernetzung von Zulieferern, Konstruktion und der Produktion immer enger wird, damit mit „vereinfachter Kommunikation" immer bessere und schnellere Ergebnisse erzielt werden können. Dies erleichtert das Abgreifen von Key Know-How in digitaler Form. Mobile Devices bringen neue Probleme, da für Hacker „i-Pad & Co" zunehmend leichte Ziele sind, und die zunehmende Nutzung von Standardsoftware in der Produktion führt zu aktuell ungelösten Problemen im Patch Management. Aus unserer Security Intelligence (X-Force) wissen wir andererseits dass die Hacker- Community regelmäßig Shopfloor Exploits veröffentlicht (inklusive der zugehörigen Pentesting Tools)

Höchste Priorität in der Produktion haben Taktzeiten und Produktionsmengen, wobei Maßnahmen für Security dies nicht beeinträchtigen dürfen. Die Anlage wird als Gesamtgewerk geliefert: Modifikationen müssen im Gesamtkontext geplant und durchgeführt werden. Das Risiko ist auch deshalb so hoch, weil das Thema Security in der Konzeptphase der Fabriken bisher keine Rolle gespielt hat.

Auch hier kann eine intergrierte SIEM-Lösung Abhilfe schaffen. Diese

Mag.

Robert Kernstock

IBM Security Solutions, Business Development Executive

ermöglicht die Überprüfung von Kommunikationspfaden, beispielsweise das Aufdecken unautorisierter Kommunikation zwischen verschiedenen Zonen innerhalb der Produktionsumgebung, zwischen Produktion und Office IT (Intranet), sowie externer Kommunikation. Das SIEM Dashboard stellt den aktuellen Security-Status dar und alarmiert automatisch im Falle von Sicherheitsbrüchen, und zwar für das Gesamtsystem ohne Unterscheidung der Produktions- und Office-IT.

Autor:

IBM Security Solutions, Business Development Executive
Jahrgang 1956, Ausbildung Betriebs- und Wirtschaftsinformatik, berufliche Erfahrung als Management Consultant und Manager in IT-Consultingunternehmen in Österreich und Zentral- und Osteuropa,bei IBM seit 2006.
Verantwortlich für Security seit 2014.

Matthias Friessnig, Alexander Pointner

FabLab, ein Maker Space an der TU Graz

Seit dem letzten Jahr betreibt das Institute of Production Science and Management gemeinsam mit dem Institut für Industriebetriebsbetriebslehre und Innovationsforschung als erste österreichische Universität ein „FabLab".

FabLabs sind Hightech-Werkstätten für die Produktion, in welchen ein reger Austausch von Know-how und Erfahrungen über spezifische Produkte und Produktionsmöglichkeiten stattfindet. Das Wort FabLab steht dabei als Abkürzung für Fabrication Laboratory. In dieser Einrichtung haben sogenannte „Maker" die Möglichkeit, unkompliziert moderne und bedienerfreundliche Produktionsmaschinen für die Prototypenfertigung nach einer kurzen Einschulung selbst und vor allem kostenlos zu nutzen. In Workshops und Seminaren treffen sich Gleichgesinnte und arbeiten gemeinsam oder alleine an Ihren Projekten. Ein FabLab ist somit ein Ort der Bildung und Wissensvermittlung.

Prof. Christian Ramsauer (li.) im FabLab Graz (Quelle: TU Graz/Lunghammer)

Am Institute of Production Science and Management und mit der Unterstützung des Institutes für Industriebetriebslehre und Innovationsforschung bei Prof. Christian Ramsauer wurde im Oktober 2014 ein derartiges FabLab an der TU Graz eröffnet. Das erste FabLab weltweit wurde 2002 von Professor Neil Gershenfield am Center for Bits and Atoms des Massachusetts Institute of Technology gegründet, welcher später die internationalen FabLab Association und die FabFoundation ins Leben rief. Nach der Eröffnung im Jahr 2014 ist die TU Graz damit die erste österreichische Universität, die ein FabLab betreibt und Mitglied der FabLab Association und der FabFoundation ist. Das FabLab Graz befindet sich am FSI in der Inffeldgasse 11 im 1. Stock in Graz und steht nicht nur allen Studierenden zur Verfügung, sondern ist jeden Donnerstag zwischen 14 und 18 Uhr auch für Privatpersonen öffentlich und kostenlos zugänglich. Neben zwei unterschiedlichen 3D-Druckern stehen den Nutzern auch ein 3D-Scanner, Laser-Cutter, Vinylcutter und eine CNC-Fräsmaschine für den privaten Gebrauch zur Verfügung. Dementsprechend ausgestattet Hightech-Werkstätten sind somit die Grundlage für die Herstellung von stark an die Kundenbedürfnisse angepassten Produkten. (weitere Informationen unter http://fablab.tugraz.at).

Erste Prototypen aus dem FabLab Graz (Quelle: TU Graz/Lunghammer)

FAB|Lab
Graz, Austria