IT-Security Live 2013 - Beherrschung von unternehmensübergreifenden IT-Infrastrukturen

Die „IT-Security live“, ein vom German Chapter of the ACM getragenes Netzwerk für Professionals aus dem Bereich des IT-Security-Managements, hat inzwischen ihren festen Stellenwert unter den Veranstaltungen des Chapters. Nach dem inzwischen zur Tradition gewordenen informellen Erfahrungsaustausch am Vorabend fand das diesjährige Treffen am 26.4.2013 im Wirtschaftsrathaus Nürnberg statt. Unter der Leitung von Dr. Jörg Schreck und seinen Mitorganisatoren Hartmut Goebel, Prof. Dr. Haio Roeckle und Gerhard Schimpf, die die einzelnen Sitzungen moderierten, widmeten sich die Teilnehmer intensiv den Impulsvorträgen und der Diskussion des hochaktuellen Themenschwerpunkts: Beherrschung von unternehmensübergreifenden IT-Infrastrukturen. Beim Austausch von hoch vertraulichen Daten zwischen Geschäftspartnern über Strukturen, deren System- und Sicherheitsmanagement in unterschiedlichen Zuständigkeiten liegt, entstehen schwer beherrschbare Risiken.

Bereits im ersten Impulsvortrag: „Das Ende des *„Luftspalts“* – Öffnung von abgeschotteten *„friendly User“* Netzen in Richtung Internet“ von *Klaus Wischnewski (DATEV eG)* wurde deutlich, in welchem Spannungsfeld sich das IT-Security-Management im rauen Unternehmensalltag bewähren muss. Einerseits müssen die Sicherheitsstandards der Unternehmens-Policy eingehalten, andererseits müssen aber aus Gründen der Arbeitseffizienz und des Wettbewerbs zunehmend die Arbeitsplätze der Mitarbeiter in einen Verbund mit Kunden und Partnern überführt werden, in dem unternehmensübergreifendende Kollaboration stattfinden kann. Weiterer Handlungsdruck entsteht aus Internet-basierten Konzepten, wie der Nutzung von Cloud-Diensten sowie der Entwicklung eigener Software Produkte unter Verwendung von Cloud und Social Media. Die vorgestellten Lösungsansätze bedingen eine sorgfältige Analyse der Bedrohungen und Risiken, die sichtbar gemacht werden müssen. Worst-case Szenarien spielen dabei eine besondere Rolle. Danach kann die Netzstruktur sukzessive in Zonen mit unterschiedlichen Sicherheitsniveaus umgebaut werden. Unternehmenskritische Informationen müssen dabei nach wie vor von den öffentlichen Netzen isoliert gehalten werden. Gleichzeitig muss im Unternehmen aber auch ein Kulturwandel stattfinden, weil durch Einsatz von Technik allein keine nachhaltige Sicherheit erreichbar ist.

Frank Jelinek (Seeburger AG) beleuchtete in seinem Vortrag die Praxis des Austauschs von großen Datenmengen mit vertraulichem Inhalt zwischen unterschiedlichsten Geschäftspartnern. In vielen Unternehmen greifen Mitarbeiter oft - sei es aus Unkenntnis oder weil es bequemer ist - zu unsicheren Umgehungslösungen. Prominente Beispiele sind öffentliche File Sharing Dienste wie Dropbox oder unverschlüsselte E-Mail Anhänge. Um diese Sicherheitsprobleme zu lösen, wurde bei Seeburger MFT (Managed File Transfer) entwickelt. Mit dieser zentralen Plattform kann im Unternehmen der gesamte Datentransfer nach hinterlegten Richtlinien abgewickelt werden, ohne dass sich der Endanwender in die Sicherheitstechnik vertiefen muss.

Eine weitere Sichtweise auf die vorgenannten Problemstellungen, Fähigkeit zur

schnellen Prozessanpassung bei Organisationsänderungen, Benutzerkomfort sowie Wahrung eines hohen Sicherheitsniveaus, beleuchtete *Michael Gerlach (Nokia Siemens Networks)* in seinem Vortrag: „Zugriffskontrolle bei unternehmensübergreifenden Geschäftsprozessen mit RBAC und Subskription“. In dem Erfahrungsbericht wird das herkömmliche RBAC Modell zur Berechtigungsvergabe insofern angepasst, dass den Benutzern lediglich Organisations-Rollen zugewiesen werden. Mit diesen sind Kataloge mit Service-Rollen verbunden, die von Benutzern subskribiert werden können. Dieser Grad an Flexibilität wird dadurch erkauft, dass sich in Einzelfällen Benutzer mehr Zugriffsrechte zuordnen können, als sie für die Durchführung einer Aufgabe benötigen. Das damit verbundene Risiko wird in der Praxis zumindest durch ein ex-post Audit begrenzt.

Die Diskussion um die Schlüsselbegriffe Vertrauen und Reputation wurde durch den Vortrag von *Mathias Muhlert (UniCredit Bank AG)* mit dem Thema „Heranziehen von Social Media-Informationen zur Einschätzung eines Partners“ eingeleitet. Muhlert zeigte beispielhaft, dass es heute eine ganze Reihe ausgereifter Tools zum professionellen Screening von firmenbezogenen Social Media Informationen gibt, die im Bereich des IT-Security-Managements ergänzend eingesetzt werden können. Je nach Fragestellung können diese defensiv zur Risikoerkennung aber auch aktiv zur Entscheidungsfindung für das Management eingesetzt werden. Diese Tools erlauben es u. a. auch die Reputation von zukünftigen Geschäftspartnern einzuschätzen, indem Rückschlüsse gezogen werden aus Äußerungen, die diese in verschiedenen Social Media über sich preisgegeben haben. Ist es ethisch gerechtfertigt diese Informationen zu verwenden? „Eine Information, die ich freiwillig den Social Media anvertraut habe, gehört nicht mehr mir persönlich. Sie ist zum Allgemeingut der Öffentlichkeit geworden. Damit darf ich sie auch verwenden“, so lautete ein Beitrag der durchaus kontroversen Diskussion.

Prof. Dr. Hans-*Joachim Hof (Munich IT-Security Research Group, Hochschule München)* zeigte in seinem Vortrag: “IT-Sicherheit und Usability – ein Widerspruch?“ anhand einiger drastischer Beispiele aus seinem Forschungsgebiet, dass ungenügende, schwer verständliche und nicht ausgereifte Benutzerschnittstellen zu Frustrationen und Fehlern führen. Selbst kommerziell verfügbare Produkte müssen dringend überarbeitet werden, um das in den Unternehmen angestrebte Sicherheitsniveau zu erreichen. Die Gruppe von Prof. Hof hat Richtlinien erarbeitet mit dem Fokus die Benutzbarkeit von Sicherheitseinrichtungen zu verbessern.

Die Tagungsteilnehmer waren sich einig, dass die IT-Sicherheit nach wie vor ein andauernder Prozess ist, der mit jedem neuen Technologieschub und mit jeder neuen bekannt gewordenen Bedrohung überdacht und angepasst werden muss. Insbesondere Professionals im Bereich des IT-Security Managements benötigen dazu branchenübergreifenden Gedankenaustausch, um – angeregt durch die Impulsreferate der Referenten – von den Erfahrungen anderer Unternehmen zu lernen und Best Practices weiterzuentwickeln.

Hinweise zur Tagung finden sich unter http://www.it-security-live.org. Dort wird auch der CfP für die Tagung 2014 veröffentlicht werden.

Gerhard Schimpf