Computerworld 14/12. August 2011
→ **www.computerworld.ch**

Gesundheits-Check für die IT

Für produzierende Unternehmen ist die IT Lebensader des operativen Geschäfts. Das macht sie sowohl zum Business Enabler als auch zum potenziell wunden Punkt. Systematische Security Audits helfen, Schwachstellen frühzeitig zu erkennen und zu beseitigen.

→ **VON DIETMAR BÖHM**

Schweizer Unternehmen, die qualitativ hochwertige Produkte herstellen, können von der Globalisierung der Märkte durchaus profitieren. Die in Stäfa beheimatete Sonova Gruppe ist dafür ein Paradebeispiel. Der führende Hersteller im Bereich Hörgeräte und Hörimplantate vereinigt diverse bekannte Marken wie Phonak, Unitron, Advanced Bionics und Sona unter einem Mantel und erreicht damit einen Jahresumsatz von über 1,6 Milliarden Schweizer Franken.

Das Interessante daran: Nur 3 Prozent davon werden auf dem heimischen Markt erwirtschaftet. Der überwiegende Teil der Kunden sitzt in Amerika, Europa oder Asien. Dieser globale Distributionsprozess kommt nicht ohne IT-Unterstützung aus. Seinen weltweiten Kunden bietet der Hörgerätehersteller zum Beispiel B2B-Lösungen an, in welche die Backend-Systeme voll integriert sind. Dass dabei sowohl der Datenschutz sensitiver Daten als auch die Sicherheit der Web- und Backend-Systeme gewährleistet sein muss, versteht sich von selbst. In Zukunft wird der Integrationsgrad zwischen Frontend-Systemen zum Kunden und der komplexen Backend-Architektur noch weiter steigen, ohne dass auf Seiten der Sicherheit Abstriche gemacht werden dürfen.

Schon das alleine ist eine komplexe Herausforderung für die IT. Eine weitere ist der besondere Produktinnovationszyklus des Unternehmens: Sonova richtet diesen primär nach den beiden wichtigen Hörgerätemessen in Europa und den USA aus, damit die neuen Produkte bereits an den Messen bestellt werden können (Show&Ship-Strategie). Die zugrundeliegende IT-Infrastruktur, die Prozesse und Daten müssen also bis zum jeweiligen Messetermin implementiert, getestet, skalierbar, lauffähig und vor allem sicher sein. Die IT ist damit eng an die Wertschöpfung des Unternehmens gekoppelt.

Dietmar Böhm ist seit 2004 Director Corporate IT der Phonak AG. Er hat die IT der Sonova Gruppe aus einer klassischen IT in eine moderne Corporate IT überführt

→ **www.phonak.com, www.sonova.com**
→ **www.oneconsult.com**

IMMER IN BEWEGUNG

Aufgrund der breiten Produktpalette, der hohen Kadenz neuer Produktangebote und verschiedener Firmenzukäufe befindet sich die IT-Infrastruktur von Sonova in stetigem Wandel. Bausteinartige, modulare Systeme und ein effizientes Change Management werden damit zu Wettbewerbsfaktoren. Dabei kommen verschiedenste Technologien und Architekturen zum Einsatz – immer unter der Prämisse der Wirtschaftlichkeit und Sicherheit.

Was die IT-Security betrifft, haben Verfügbarkeit, Vertraulichkeit und Integrität gleich hohe Priorität. Vorgabe ist, sowohl die Geschäftsprozesse zuverlässig zu unterstützen als auch die Einhaltung betriebsinterner Richtlinien sowie nationaler und internationaler gesetzlicher Regularien zu gewährleisten.

«IT Security Audits setzen zwingend Fachkompetenz, Erfahrung und Neutralität voraus»
Dietmar Böhm

REGELMÄSSIGE SICHERHEITSTESTS

Um alle diese Vorgaben erfüllen zu können, unterziehen wir alle Business-relevanten IT-Komponenten regelmässigen Security Audits, unabhängig davon, ob diese intern oder von einem externen Partner betrieben werden. Dies ist zwingender Bestandteil des Change-Management-Prozesses.

Obwohl die Security Audits nur einen Bruchteil der Implementierungs- und Betriebskosten ausmachen, ist die Wahl des richtigen externen Anbieters entscheidend. Die wichtigsten Kriterien sind: hohe Fach- und Sozialkompetenz, eingespielte Projektteams, nationale und internationale Projekterfahrung, tadelloser Ruf, Zuverlässigkeit, Bekanntheitsgrad, Methodenkompetenz und nicht zuletzt Produkteneutralität. In Bezug auf das Risikomanagement darf die Fachkompetenz auch nicht auf einzelne wenige Köpfe konzentriert sein. Insbesondere grössere Anbieter sind meist nicht produkteunabhängig und/oder verwenden Audits gerne zur Zusatzauftragsgenerierung. So macht es wenig Sinn, den Lieferanten eines Systems auch mit dessen Auditierung zu beauftragen. Ebenso wenig ist es sinnvoll, wenn sich die IT selbst auditiert.

Auf der Suche nach dem passenden Partner hörte sich die Sonova-IT im «Kollegennetzwerk» bei befreundeten Firmen um, schlug bei den einschlägigen Fachmedien nach und liess sich schliesslich von drei Anbietern konkrete Angebote machen. Nach eingehender Prüfung fiel Anfang 2009 die Entscheidung für den Sicherheitsspezialisten OneConsult aus Thalwil.

Seither werden alle Plattformen vor deren Inbetriebnahme und nach massgeblichen Veränderungen konsequent auditiert – in der Regel halbjährlich. Nach kurzer Einführung in die Systemlandschaft testen die Spezialisten von OneConsult selbstständig.

METHODE UND ANSATZ

Die Sonova-Systemarchitektur richtet sich weitestgehend nach dem Open-Source-Referenzmodell TOGAF (The Open Group Architecture Framework). Die meisten Applikationen sind nach dem Multi-Tier-Ansatz aufgebaut. Dies ermöglicht die gemeinsame Nutzung von Tiers, die Auslagerung einzelner Komponenten in die Cloud und die rasche Anbindung künftiger Applikationen dank standardisierter Schnittstellen bzw. Module. Ein weiterer Vorteil ist, dass nicht mehr so viele Applikationen komplett überprüft werden müssen. Aufgrund der gemeinsamen Nutzung von Komponenten kann mit dem gleichen Projektbudget intensiver nach Sicherheitslücken gesucht und die entsprechende Applikation schneller ausgeführt werden.

OneConsult stellt die Testerteams aufgrund der zu prüfenden Systemtypen zusammen. Je nach Systemtyp und Anforderung kommen Penetration-Tests, Application Security Audits, Proof-of-Concept-Tests (Ethical Hacking) oder ein Mix aus allen vorgenannten Testtypen zur Anwendung. Um das Security-Benchmarking zu vereinfachen, werden die technischen Audits nach dem De-Facto-Standard OSSTMM (Open Source Security Testing Methodology Manual) durchgeführt. Bei Web Application Security Audits werden zusätzlich die Empfehlungen des «Open Web Application Security Project» (OWASP) berücksichtigt.

Nach Abschluss der Tests bespricht das Projektteam, bestehend aus Sonova- und OneConsult-Mitarbeitern, den Befund und setzt zeitnah entsprechende Massnahmen um. Gefunden wird dabei so gut wie immer etwas, vor allem nach grösseren Changes. Meist handelt es sich dabei um Flüchtigkeitsfehler, zum Beispiel übersehene Sicherheits-Updates auf einzelnen Servern, von denen die Sonova-IT immerhin an die 700 betreut. Weitere typische Sicherheitswarnungen betreffen etwa den Sicherheitsgrad von Passwörtern. Aber auch schwerwiegendere Lücken, zum Beispiel die Verwundbarkeit für Crossite-Scripting-Angriffe oder einer Schwäche im SSL-Protokoll, kommt man so auf die Spur. Oft lassen sich solche Lücken recht schnell schliessen – in letzterem Fall etwas durch ein simples Update auf SSL Version 3 – nur aufspüren muss man sie dazu rechtzeitig. Die «segregation of duty», also die strikte Trennung zwischen Programmierer- und Testerdienstleister, hat sich hier sehr bewährt. Zum einen aus Kostengründen, zum anderen aber auch, weil dann keine Interessenskonflikte bestehen.

FAZIT: NEUTRALE SICHT IST GEFRAGT

Business-kritische Applikationen sollten regelmässig von kompetenten Security-Auditoren auf ihre Sicherheit hin überprüft werden. Bei der Wahl des Anbieters müssen nicht nur die fachlichen Kriterien, sondern auch das Bauchgefühl berücksichtigt werden. Mit dieser Strategie war Sonova in den letzten Jahren bisher sehr erfolgreich. So können wir sicher sein, dass der Nutzen für unser Unternehmen und eine neutrale, umfassende Auditierung der Systeme im Vordergrund stehen – und nicht ein möglichst hohes Projektbudget. ←

Projektumfang und -aufwand

Scope	ca. 1 Dutzend Applikationen und verschiedene Infrastrukturdienste
Tests	Application Security Audits, Penetration Tests und Ethical Hacking, Client Security Checks, E-Mail-Security-Checks
Projektdauer	Start der Zusammenarbeit: Frühling 2009, fortlaufende (Teil-)Projekte
Aufwand	ca. 30 Tage/Jahr extern ca. 30 Tage/Jahr intern
Beteiligte Personen	→ 8 Personen extern (pro Teilprojekt 1 bis 4 Personen: 1 bis 3 Tester – inkl. Projektleiter – plus 1 Person zur Qualitätssicherung) → 5 Personen intern (je 1 Person für Infrastruktur & Netz, SAP PI, Web, SFDC sowie für die Projektleitung)