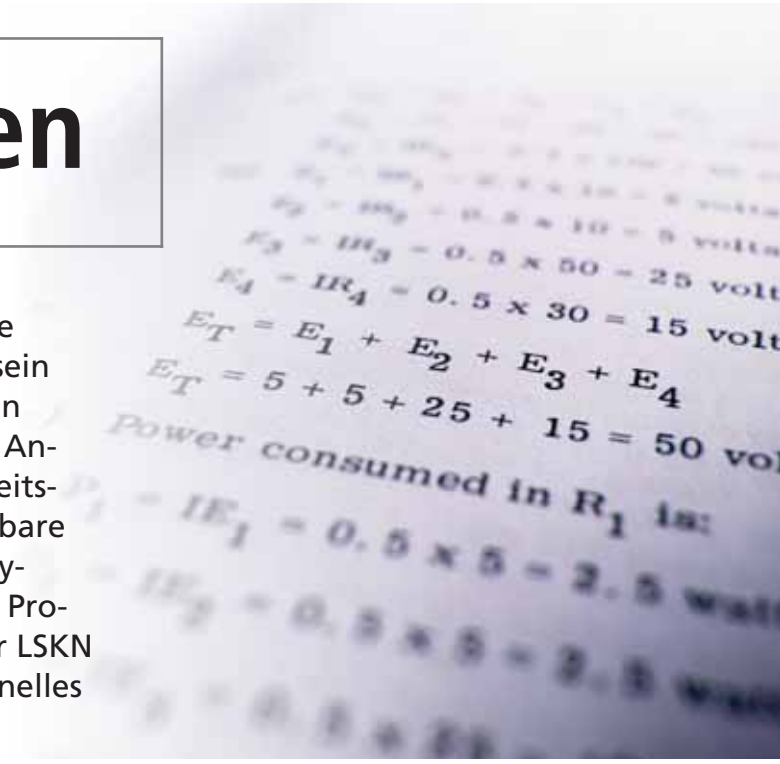
IT-Sicherheit

Welt der Zahlen



Der Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) erweitert sein IT-Sicherheitsmanagement um ein Security Level Management. Die Anwendung überprüft den Sicherheitsstatus aller IT-Systeme, legt messbare Ziele für die Leistung der Security-Applikationen fest und definiert Prozesse, um diese zu erreichen. Der LSKN will so die Basis für ein professionelles Security Management schaffen.

Der LSKN will damit die IT-Sicherheit permanent optimieren, seine Datenschätze optimal schützen und seine Risiken minimieren. Bereits zu Beginn der Erweiterung konnte der LSKN bedeutende Verbesserungen erzielen.

3.075 Euro verdient ein Arbeitnehmer aktuell durchschnittlich in Niedersachsen, der Verbraucherpreisindex ist von Mai 2009 bis Mai 2010 um 1,4 Prozent gestiegen und im Jahr 2060 werden dort nicht nur 200 über 100 Jahre alte Menschen leben, sondern mehr als 15.000. Das alles und noch viel mehr – um genau zu sein über 80 Millionen Statistikdaten – steckt in der größten regionalstatistischen Datenbank Deutschlands, die der LSKN bereitstellt. Neben der Funktion als Statistikzentrale ist der in Hannover ansässige Landesbetrieb auch IT-Dienstleister und betreibt als solcher die Systeme einiger Landesministerien und nachgeordneter Verwaltungen. Dem LSKN sind also nicht „nur" die rund 1.000 eigenen PC-Systeme anvertraut, sondern insgesamt etwa 10.000 PCs und Server.

„Trotz der vielen Angriffspunkte ist es uns bisher gelungen, Negativschlagzeilen vom LSKN fern zu halten", so Michael Schätzke, stellvertretender IT-Sicherheitsbeauftragter. „Damit das so bleibt, optimieren wir derzeit unsere Prozesse des IT-Sicherheits- beziehungsweise Verwundbarkeits-Managements", erklärt der Sicherheitsverantwortliche, der auch die neue Rolle des IT-Vulnerability-Managers übernommen hat. „Uns war klar, dass unsere Prozesse umso effizienter sein würden, je früher wir Schwachpunkte in der Systemlandschaft identifizieren und beseitigen können", sagt Schätzke. „Wenn diese erst durch einen Vorfall evident werden, kann auch der beste Prozess nur noch Schäden begrenzen."

Deshalb begann man Ende 2009 mit der Suche nach einem Werkzeug zum Security Information Event Management, das Schwachpunkte aufspüren sollte. Der LSKN versprach sich von dem Tool mehr Transparenz, welche die Grundlage für die Neudefinition von Policies und Leistungszielen für IT-Sicherheitstechnik und -prozesse bilden sollte.

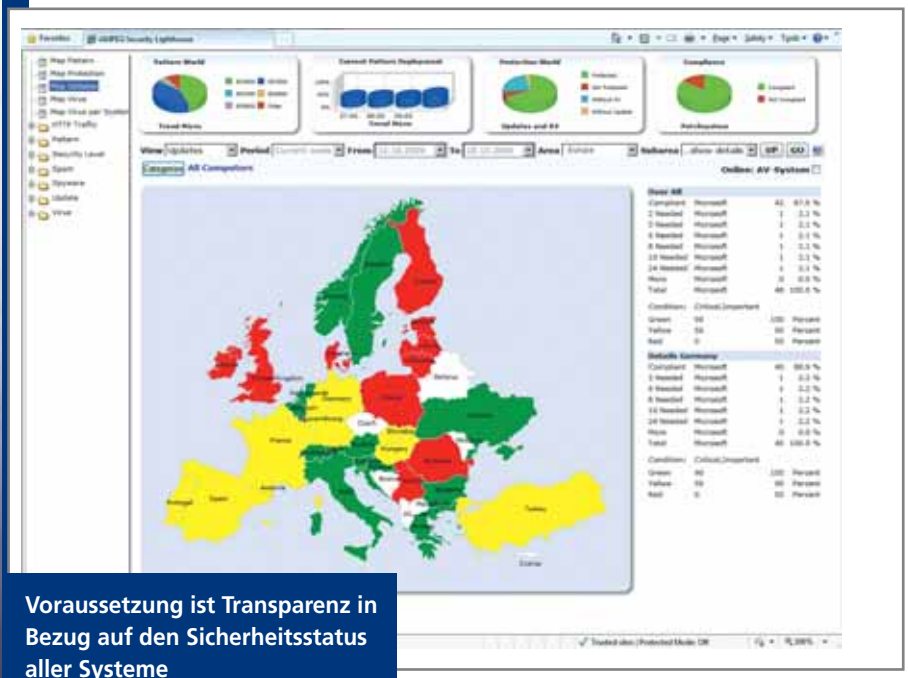
Schnelle Inbetriebnahme

Das Ampeg Security Lighthouse ist eine herstellerunabhängige Monitoring- und Reporting-Software. Die webbasierende Anwendung führt aktuelle Informationen aus den verschiedenen Sicherheitsapplikationen in einer zentralen Konsole zusammen.

Nachdem das Tool evaluiert, nach einem positiven Urteil beschafft und installiert war, übergab man die Sicherheitslösung an das IT-Sicherheitsmanagement-Team mit Michael Schätzke, der sich zusammen mit Michael Hänsel, Senior Development Consultant bei Ampeg, im Januar daran machte, die Log-Datenbanken der Sicherheitssysteme an das Security Lighthouse anzuschließen. Der LSKN verfügt über mehrere Microsoft WSUS-Server für das Patch Management sowie mehrere Anti-Malware-Server zum Schutz der PCs, Server sowie eMail-Postfächer. Nach vier Wochen war der Anschluss der ersten Systeme erledigt – inklusive der Integration einer neuen Schnittstelle für die F-Secure Virenschutzsoftware. Die Integration der restlichen Server konnten die Techniker des LSKN ab diesem Punkt selber übernehmen.

In Security Lighthouse wird der Sicherheitsstatus der gesamten Systemlandschaft mittels Ampelfarben in einer Security Information Map angezeigt. „In der Gesamtsicht sind Sicherheitslücken viel leichter zu identifizieren", so Schätzke. Schon unmittelbar nach der Inbetriebnahme des Monitorings

Strategisches Security Level Management



Voraussetzung ist Transparenz in Bezug auf den Sicherheitsstatus aller Systeme

konnten erste Verbesserungen in Bezug auf die Sicherheit eingeleitet werden. Einige Rechner verfügten beispielsweise nicht über aktuelle Versionen der Antimalware-Software, was nicht ohne Weiteres zu erkennen war. Hier wurden Updates initialisiert.
Ebenso konnten unmittelbar die Rechner identifiziert werden, die Betriebssystem-Updates nicht erhalten hatten. Auch hier wurde sofort mit dem gezielten Schließen der Sicherheitslücken begonnen.
„Außerdem haben wir noch Rechner gefunden, die den falschen Update-Servern zugeordnet worden waren", erzählt Schätzke. „Die mussten manchmal länger auf ihr Update warten, als eigentlich nötig gewesen wäre. Mit Security Lighthouse konnten wir alle Systeme aufgrund ihrer standortbezogenen IP-Adressen richtig zuordnen."

Aktives Reporting

Mit der Inbetriebnahme des Monitorings ist das Sicherheitsteam nun in der Lage, regelmäßig Reports zur Sicherheitslage für das Management zu erstellen. „Wenn früher eine Anfrage kam, wie gut wir gegen einen aktuell in der Presse vertretenen Virus geschützt waren, hat es im schlimmsten Fall 14 Tage gedauert, bis wir die Informationen zum Rollout-Status des betreffenden Sicherheits-Patches oder –Patterns zusammengetragen hatten", blickt Schätzke zurück und erzählt, dass es bisher sehr aufwendig und zeitintensiv gewesen war, die notwendigen Details aus den einzelnen Konsolen der Management-Systeme – eine übergeordnete Konsole für alle Systeme gab es bisher nicht – zu extrahieren.
„Das Security Lighthouse hingegen zeigt Gesamtsicht und Details in nahezu Echtzeit und sagt uns außerdem, welche Updates den Rechnern fehlen", so Schätzke. „Die Details geben wir zur Unterstützung bei der Fehlerbehebung an unsere Admins weiter, die Auswertung der Gesamtlage an das Management. Das Security Lighthouse schlägt hier eine Brücke zwischen Technik und Management und liefert beiden die Informationen die sie brauchen – in der Sprache, die sie verstehen."
In die Management-Reports sollen in Zukunft auch Trendanalysen zu den Update-Vorgängen einfließen, durch die sich zeigen lässt, wie das Gesamtniveau der IT-Sicherheit steigt.

Gesteigertes Schutzniveau

Aktuell wird die Verbesserung des Schutzniveaus vom Rechenzentrum aus vorangetrieben, wo die Monitoring-Lösung bislang läuft. Weil noch kein Berechtigungsmodul für ein Rollenmanagement übernommen wurde, unterstützt das Kernteam die Administratoren in den Fachabteilungen mit Hinweisen zu Sicherheitslücken. Im nächsten Schritt soll den Dienststellen selbst Zugriff auf die Schwachstellenanalyse für ihre spezifischen Bereiche ermöglicht werden.
„Wir steigern die Transparenz und erleichtern unserem Team so die technische Optimierung unserer Schutzstrukturen", erklärt Schätzke. „Das soll nicht heißen, dass wir aktuell nicht gut geschützt sind – Malware-Vorfälle kamen so gut wie nicht vor – aber nun können wir die Verbesserungen schwarz auf weiß belegen, haben Messwerte und Zahlen, die wir auch an das Management weitergeben können. Ein gutes Bauchgefühl in Bezug auf den Sicherheitsstatus wurde ersetzt durch exaktes Wissen."

Hilfe zur Strategiebildung

Die Messdaten zur Leistung der Sicherheitssysteme – etwa zur Dauer eines Update-Rollouts – nutzt das IT-Sicherheitsmanagement als Grundlage, um Vorgaben, Ziele und Prozesse zu optimieren.
„Security Lighthouse hilft uns nachzuvollziehen, wie lange Rollouts wirklich dauern und welche Vorgaben schließlich technisch und organisatorisch realistisch sind", erläutert Schätzke.
„Verzögerungen bei Updates sehen wir sofort und können die Gründe eruieren." Bei der Bestimmung der Ziele spielen viele weitere Faktoren eine Rolle, zum Beispiel wie gut ein bestimmter Netzwerkabschnitt geschützt sein muss oder wie die Vorgaben bezüglich der Hochverfügbarkeit sind. Am Ende will der LSKN konkrete Grenz- und Schwellenwerte für Patch- und Pattern-Rollouts für alle Bereiche festlegen und diese bei jedem Rollout automatisiert gegen die tatsächliche Leistung der Systeme prüfen lassen. Dieses Security Level Management stellt eine Qualitätssicherung für die IT-Sicherheit dar und trägt wirksam zur Risikominimierung bei.
„Ich denke, unsere Bilanz nach sechs Monaten kann sich sehen lassen", resümiert Michael Schätzke. „Wir haben die Grundlage für ein professionelles Security Level Management geschaffen und bereits wichtige Verbesserungen der IT-Sicherheit erzielen können. Die zahlenbasierenden Steuermöglichkeiten zahlen sich schon aus." **mk**