Veröffentlicht am: 25.08.2007

RedTeam Pentesting GmbH: IT-Sicherheit aus Sicht des Managements - ein Kostenpunkt ohne direkten Return On Investment

Autor: Claus Overbeck

Es gibt keine IT-Sicherheit ohne organisatorische IT-Sicherheit. Technische IT-Sicherheit ist die eine Seite und die organisatorische IT-Sicherheit die andere Seite. Was sind Ihre Erfahrungen mit den Kunden?

In den letzten Jahren herrschte die Mentalität vor, dass IT-Sicherheitsprobleme alleine durch den Einsatz der richtigen Appliance erschlagen werden können. Hierbei entwickelte sich regelmäßig ein technischer Tunnelblick, gefördert durch die Werbeaussagen der Hersteller von Sicherheitslösungen, die ihre Produkte als Allheilmittel für alle Sicherheitsprobleme vermarkten. Heute hat sich das Bild ein wenig gewandelt: IT-Sicherheit wird als ganzheitlicher Prozess erkannt.

Zu einem Sicherheitsmanagement gehören eine Vielzahl durchdachter und überprüfter Workflows. So muss zum Beispiel die Personalabteilung die IT über Mitarbeiter informieren, welche das Unternehmen verlassen. Gleichzeitig muss auch die IT-Abteilung einen Überblick haben, für welche Systeme diese Mitarbeiter Zugänge hatten. Für solche organisatorischen Prozessabläufe finden sich noch zahlreiche weitere Beispiele.

Die Kunden der RedTeam Pentesting GmbH wählen hier eine ganzheitlichen Ansatz. Sie definieren Schutzziele von wirtschaftlicher Relevanz und lassen überprüfen, inwiefern die technischen und organisatorischen Maßnahmen ausreichend sind, um einen erfolgreichen Angriff in der Praxis abzuwehren.

Zusammenhang zwischen Geschäftspolitik und IT-Sicherheitspolitik. Klaffen hier große Lücken? Wie können Sicherheitsexperten das Management von der Wichtigkeit der Maßnahmen überzeugen? Man spricht zwei Sprachen!

Das Problem bei der Bewilligung von Mitteln für Sicherheitsmaßnahmen liegt darin, dass die IT-Sicherheit aus Sicht des Managements ein Kostenpunkt ohne direkten Return On Investment ist. Stattdessen stellt IT-Sicherheit eine Maßnahme dar, das Risiko potentieller Schäden durch IT-Sicherheitsvorfälle zu vermindern. Die reelle Gefahr, die von Einbrüchen in IT-Systemen ausgeht, wird jedoch noch viel zu sehr unterschätzt. Dies liegt sicherlich auch daran, dass die Folgen eines solchen Einbruchs für den Betrachter nicht in der Form greifbar sind, wie sie es auf einer physischen Ebene wären.

Wird im Büro des Geschäftsführers der Tresor aufgebrochen und die darin liegenden Dokumente entwendet, so ist der Verlust sichtbar. Ein geschickter Einbruch in IT-Systeme wird jedoch weitestgehend unbemerkt bleiben. Welche Dokumente kopiert wurden, ist zudem meist nicht nachvollziehbar. Man bewegt sich auf einer Ebene, auf welcher die Vorstellungen über die Ausmaße eines solchen Einbruchs meist hinter den reellen Folgen zurückbleiben. So werden Budgetforderungen oft mit dem altbekannten "bisher ist doch auch nichts passiert" verworfen.

Hierbei ist dem Management nicht vollends bewusst, welche Risiken im Bereich IT eingegangen werden. Die gleichen Dokumente, welche als Ausdruck im Safe eingeschlossen werden, werden im Netzwerk auf IT-Systemen gespeichert, deren Sicherheit um ein Vielfaches komplexer ist als die eines Tresors. Gelingt es den Testern in einem Penetrationtest sich Zugang zu diesen Dokumenten zu verschaffen, kann dies die IT-Sicherheitsrisiken für das Management greifbar machen.

Verantwortung für IT-Sicherheit - Wer hat sie?

Die Verantwortung für die Sicherheit der IT ist ein Thema, welches in vielen mittelständigen Unternehmen nicht ausreichend geklärt ist. Zwar wird häufig einer Person diese Aufgabe zugeteilt. In der Praxis kann diese aber selten ihre Vorstellungen komplett durchsetzen, da sie oft nicht mit ausreichenden Mitteln und Befugnissen von ihren Vorgesetzten ausgestattet sind. Hierdurch wird wieder ein Teil der Verantwortung zurück auf diese Vorgesetzten übertragen. Eine Prüfung der eigenen Sicherheitsmaßnahmen durch Dritte und das Beseitigen gefundener Mängel kann dieses Problem deutlich entschärfen.

Welche Verfahren zur Messung der IT-Sicherheit im Unternehmen gibt es?

Wir unterscheiden hier grundsätzlich zwei Verfahrensweisen: Einen (Sicherheits-) Audit und einen Pentest. Bei einem Audit wird typischerweise geprüft, inwiefern ein System die Kriterien einer meist standardisierten Checkliste erfüllt. So soll die IT-Sicherheit messbar und vergleichbar gemacht werden. IT-Systeme sind eine vergleichsweise komplexe Technologie. Dies führt dazu, dass diese Checklisten niemals vollständig sein können. Insbesondere bleiben oft Probleme unberücksichtigt, die durch das Zusammenspiel verschiedener Komponenten entstehen. Gleiches gilt für eigen entwickelte Komponenten, welche sich nur schlecht in ein standardisiertes Testverfahren pressen lassen.

RedTeam Pentesting bietet eine andere Testmöglichkeit: Die Überprüfung aus der Angreiferperspektive. Bei einem Penetrationtest versuchen die Tester das IT-System erfolgreich anzugreifen. Durch diese sehr praxisnahe Testvariante wird eine realistische Beurteilung möglich. Aussagen über die Sicherheit des IT-Systems hängen hier insbesondere von der aufgewandten Zeit aber natürlich auch von der Expertise des Pentestingteams ab. Der Penetrationtest liefert auch Aussagen außerhalb von Checklisten, wie z.B. zu eigenen Entwicklungen. Durch die völlig andere Herangehensweise bei Audits und Pentests ergänzen sich die beiden Verfahren.

Harte Fakten durch Penetrationstests? Wie wird überprüft?

Noch bevor der eigentliche Pentest stattfindet, führt RedTeam Pentesting ein Vorgespräch mit dem potentiellen Auftraggeber. Ziel dieses Gesprächs ist es, sich einen Überblick über den Bedarf des Kunden zu verschaffen, Möglichkeiten der Testgestaltung zu besprechen und Angriffsziele zu definieren. Dies könnten z.B. gespeicherte Kreditkarteninformationen der Kunden eines Webshops oder auch aktuelle technologische Weiterentwicklungen eines neuen Produkts auf dem Weg zur Marktreife sein. Durch das Vorgespräch sind die Pentester in der Lage, einen sinnvollen Testaufwand abzuschätzen und den Kunden beratend zur Seite zu stehen, welcher Testablauf am sinnvollsten ist. Der eigentliche Ablauf des Pentests ist, wie oben erwähnt, weitestgehend individuell gestaltet. Das konkrete Vorgehen im Pentest wird stark von den vorgefundenen Systemen und Gegebenheiten beeinflusst.

Die Pentester verhalten sich hierbei wie ein echter Angreifer und untersuchen die Zielsysteme auf mögliche Angriffsvektoren. Diese werden dann gezielt ausgenutzt, um in die Systeme einzudringen. Das Vorgehen, gefundene Auffälligkeiten und erfolgreiche Angriffe werden in einem Testbericht dokumentiert. Hierdurch sollen die Schwachstellen, aber auch die Angriffe für die technischen Mitarbeiter des Kunden verständlich gemacht werden. Eine Zusammenfassung in Form eines Managementkurzberichts liefert außerdem den Nicht-Technikern einen Überblick über die aktuelle Situation und Entscheidungsgrundlagen für die zu treffenden Maßnahmen.

Was wird überprüft?

Wir unterscheiden grundsätzlich zwei Arten von Penetrationtests: Zum Einem gibt es den klassischen Netzwerktest, bei dem die IT eines Unternehmens getestet wird. Die Tester versuchen hier von unterschiedlichen Ausgangspunkten, zum Beispiel von außen oder aber mit den Rechten eines interner Mitarbeiter, festgelegte Ziele zu erreichen. Üblicherweise wird versucht Zugriff auf geschützte Netzwerkbereiche und Daten zu erlangen. Als zweiten Testtyp gibt es den Produktpentest. Hierbei wird ein einzelnes System oder IT-Produkt gezielt aus der

Angreiferperspektive getestet. Dies wird häufig vor der Markteinführung eines neuen Produkts als Teil der Qualitätssicherung durchgeführt. Typische Beispiele hierfür sind Systeme aus dem Bereich Online-Banking und -Bezahlung.

Wer wird überprüft?

Durch das Ansteigen der IT-Sicherheitsvorfälle in den letzten Jahren hat nahezu jedes Unternehmen, welches IT-Systeme einsetzt, einen erhöhten Schutzbedarf. Inzwischen nutzen auch viele Mittelständler Penetrationtests, um die richtigen Ansatzpunkte zur Verbesserung ihrer Sicherheit zu ermitteln. Im Bereich Produkttest planen sogar Kleinstunternehmen Penetrationtests in das Entwicklungsbudget ein, sofern das Produkt sicherheitskritische Komponenten enthält.

Oft herrscht die falsche Vorstellung, dass bei einem Pentest die Arbeit der Administratoren auf den Prüfstand gestellt wird. Den Pentestern ist jedoch keinesfalls daran gelegen, die Arbeit einzelner Personen zu beurteilen. Vielmehr sollen die Administratoren in ihrer Arbeit unterstützt werden. Eine Sicherheitsüberprüfung durch unabhängige Experten hilft oft, dem Management die Gefahren greifbar zu machen und so auch dazu zu bewegen die nötigen Ressourcen für die IT-Sicherheit freizugeben. Die Anfragen der eigenen Leute verhallen oft ungehört.

Welche/n Vorteil/e und Nutzen hat der Kunde?

Der Penetrationtest liefert viel mehr als nur eine Liste gefundener Schwachstellen. Zu jeder Sicherheitslücke werden im Abschlussbericht Lösungsvorschläge aufgezeigt, die die Best Practices wiedergeben. So wird der Kunde nicht nur mit seinen Problemen konfrontiert, sondern vielmehr ein direkter Beitrag zur Verbesserung der IT-Sicherheit geleistet. RedTeam Pentesting sieht sich hier nicht als "Gegner" der Administratoren sondern als Partner, der in Zusammenarbeit mit dem Management und den Technikern die Sicherheit des Unternehmens stärkt.

Durch die Vorstellung der Testergebnisse und die Demonstration der gefundenen Sicherheitslücken in einer Abschlusspräsentation wird ein hoher Schulungseffekt und eine Verbesserung des Problembewusstseins bei den Mitarbeitern erreicht. Das Resultat ist eine nachhaltige Steigerung des Sicherheitsniveaus.

Claus Overbeck, Geschäftsführer
RedTeam Pentesting GmbH
