

Editorial

## „Besonders intensive Prüfung ...“,

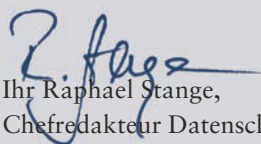
liebe Leser,

für einen großen Teil der Bevölkerung? Dies stellt das Bundesinnenministerium in einer Stellungnahme zum ePass in Aussicht. Wird ein solcher Pass von den Kontrollsystemen zukünftig nicht erkannt, müssen die Grenzer den Betroffenen einer „besonders intensiven“ Kontrolle unterziehen, so das BMI auf unbehagliche Fragen des Chaos Computer Clubs (siehe [www.ccc.de/epass/stellungnahme-bmi](http://www.ccc.de/epass/stellungnahme-bmi)).

Und die Wahrscheinlichkeit, dass ein biometrischer Pass zurückgewiesen wird, ist nicht gering: Zum einen funktionieren die Erkennungssysteme nicht wirklich zufrieden stellend, zum anderen ist nicht sicher, dass RFID-Chips überhaupt zehn Jahre durchhalten und nicht vorher ihren Geist aufgeben. Und dann hätten wir da noch einen Teil der Bevölkerung, dessen biometrische Merkmale per se schlecht zu erfassen sind. Details lesen Sie auf Seite 9.

In all diesen Fällen stünde der Betroffene ab 2007, wenn der RFID-Chip neben dem digitalen Foto auch den Fingerabdruck speichert, ziemlich dumm vor der Passkontrolle da ...

Ein frohes Weihnachtsfest wünscht

  
Ihr Raphael Stange,  
Chefredakteur Datenschutz PRAXIS

### Microsoft-Tool zur IT-Risiko-Selbsteinschätzung

# Selbsterkenntnis ist der erste Schritt zur Besserung

Sie möchten wissen, wie es um die IT-Sicherheit in Ihrem Unternehmen bestellt ist? Das Microsoft-Tool MSRSAT bietet eine Analyse, die den aktuellen Stand abschätzt und beurteilt. Es fasst die Ergebnisse abschließend in einem Bericht zusammen – sehr praktisch, um z.B. gegenüber der Geschäftsleitung die Notwendigkeit, Sicherheitslücken zu schließen, zu untermauern.

► In den Unternehmen gehören Risiken als solche oft nicht zu den wichtigsten grundsätzlichen Problemen. Kritisch ist vielmehr ein mangelndes oder gar fehlendes Risikobewusstsein.

Dies gilt in besonderem Maße für den Betrieb von IT-Systemen. Zwar ist das Wissen um Bedrohungen für die IT-Sicherheit in den letzten Jahren enorm gestiegen. Doch klaffen noch immer mehr oder weniger große Lücken in den Schutzmaßnahmen.

### Risiken aufspüren und beherrschbar machen, das Risikobewusstsein bei den Mitarbeitern erhöhen

Microsoft bietet dazu ein ganzes Bündel von Werkzeugen, Maßnahmen und Informationen, das den Unternehmen hilft, ihre Risiken zu ermitteln und das Risikobewusstsein sowie den Schutz der Unternehmens-IT zu erhöhen.

### Sicherheitslücken in den wichtigen Unternehmensbereichen erkennen

Unter dem sperrigen Titel MSRSAT (Microsoft Security Risk Self-Assessment) bietet Microsoft seit Oktober ein Tool zur Selbstanalyse an. Das Programm testet Ihre IT-Sicherheitseinrichtungen auf ihre Wirksamkeit. Es orientiert sich unter anderem an den anerkannten Standards des IT-Grundschutzes vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und an der ISO 17799.

Auf der Basis Ihres Geschäftsprofils, das Sie eingeben müssen, überprüft das Programm, welche Risiken für Ihr

Unternehmen in den folgenden Bereichen existieren:

- Infrastruktur
- Anwendungen
- Betriebssicherheit
- organisatorische und physische Sicherheit

Insgesamt dauert der Sicherheits-Check zirka eine Stunde. Er ist ein erster Schritt zur Umsetzung eines optimierten Sicherheitskonzepts. Zudem bietet das Tool Empfehlungen

Überblick	
<input checked="" type="checkbox"/>	<b>Einleitung</b> Über die Risikoeinschätzung
<input type="checkbox"/>	<b>Geschäftsrisikoprofil</b> (10 Min) Ihre Sicherheitsrisiken als Geschäftstätigkeit
Analysebereiche	
<input type="checkbox"/>	<b>Infrastruktur</b> (10 Min) Einsatz von IT-Security-Komponenten und Systemen
<input type="checkbox"/>	<b>Anwendungen</b> (10 Min) Ihre kritischen Anwendungen und wie gut sie geschützt sind
<input type="checkbox"/>	<b>Betrieb</b> (10 Min) Prozess- und Vorschriftsrichtlinien, welche die Sicherheit verbessern
<input type="checkbox"/>	<b>Organisatorische &amp; Physische Sicherheit</b> (10 Min) Allumfassende Sicherheit im Unternehmen
Ergebnisse	
	<b>Zusammenfassung der Ergebnisse</b> Überblick über ihre Auswertung
	<b>Bericht</b> Ein vollständiger Bericht

### Die Schritte der Selbstanalyse

und Informationen über Industrie-Sicherheitsstandards.

### So installieren Sie das Tool

Nach dem Start der Installationsroutine haben Sie die Wahl zwischen zehn Sprachvarianten – was für global operierende Unternehmen interessant sein dürfte, deren Firmenzentrale oder Entscheidungsträger z.B. in Schweden oder England sitzen.

Die Installationsprozedur prüft, ob die notwendigen Anwendungsvoraussetzungen vorhanden sind. Die .NET-Anwendung auf C# und XML benötigt

- Windows 2000 oder XP,
- Internet Explorer 6.0 und
- Microsoft.Net Framework 1.1.

**Tipp:** Laden Sie vorher die .NET-Komponenten über den Microsoft-Update-Server auf Ihren Rechner und spielen Sie – falls noch nicht geschehen – die aktuellsten Service Packs ein.

### Der Auftakt: allgemeine Informationen

Die Anwendung fragt in der Einleitung zunächst allgemeine Informationen ab, die ein DSB noch allein verantwortlich beantworten kann.

Bei den einzelnen Fragepunkten findet sich in der Regel noch ein ?-Button. Stellen Sie Ihren Mauszeiger auf das Symbol, erhalten Sie zusätzliche Informationen zum abgefragten Thema.

### Entscheiden Sie, ob Sie Ihre Daten zu Vergleichszwecken zur Verfügung stellen wollen oder nicht

Microsoft schlägt Ihnen in diesem Abschnitt auch vor, die Ergebnisse Ihrer Analyse in anonymisierter Form anderen Nutzern zur Verfügung zu stellen, um ihnen einen Vergleich zu ermöglichen. Dies bleibt jedoch jedem Anwender selbst überlassen. Markieren Sie im Zweifelsfall „Nein, danke“, um eine spätere Datenübertragung zu unterbinden.



**Sind Sie nicht Datenschutzbeauftragter und Admin in Personalunion, arbeiten Sie am besten mit einem IT-Verantwortlichen zusammen.**

### Erstellen Sie das Risikoprofil gemeinsam mit einem IT-Verantwortlichen

Ziehen Sie ab Stufe 2 unbedingt einen IT-Verantwortlichen hinzu, der die fachspezifischen Fragen in Zusammenarbeit mit Ihnen beantwortet.

Zur Beurteilung des geschäftsbedingten Risikos ermittelt MSRSAT die Kernbereiche Ihrer Organisation. Geschäftsrisiko, Technologie, physische und organisatorische Sicherheitsmaßnahmen werden in fest umrissenen Analysebereichen evaluiert.

### Ein abschließender Report zeigt, wo Ihr Unternehmen steht

Nach der Beantwortung der etwa 50 Fragen erstellt das Programm für Sie eine umfangreiche Auswertung im HTML-Format.

Es erzeugt für jeden Analysebereich einen Geschäftsrisikoindex (BRP – Business Risk Profile) und einen so genannten Verteidigungsindex (DiD – Defense-in-Depth) Ihrer Organisation. Die Zusammenfassung der Ergebnisse und die Bewertung der grafischen Darstellung werden ausreichend erläutert.

### Sie erhalten Vergleiche mit anderen Unternehmen und Verbesserungsvorschläge

Die mehr als 20-seitige Auswertung enthält für jede Kategorie der einzel-

nen Analysebereiche eine Beschreibung der „best practice“, sodass Sie Ihr Unternehmen an den Besten am Markt messen können, sowie Vorschläge zur Behebung eventueller Mängel in Ihrem Betrieb.

Die Spalte „Empfehlungen“ bietet weitere Vorschläge zur Verbesserung des derzeitigen Zustands.

### Fazit: einfache Anwendung, nützliche Ergebnisse

Für Datenschutz- und Datensicherheitsbeauftragte ist das MSRSAT-Tool eine einfache und effiziente Möglichkeit, sich in relativ kurzer Zeit einen Überblick zu verschaffen. Stellt MSRSAT Defizite fest, haben Sie schwarz auf weiß eine Argumentationshilfe in der Hand, mit der sich Nachbesserungen begründen lassen.

### Führen Sie die Analyse in Abständen durch, ergibt sich eine Tendenzanalyse

Das Diagnosetool können Sie auch wiederholt nutzen. Ein Vergleich der berechneten Index-Werte zeigt, ob Sie Fortschritte auf dem Weg zur Risikominimierung in Ihrer Firma erzielt haben. Lassen sich positive Veränderungen feststellen, beweist das den Erfolg Ihres Einsatzes.

*Hermann Keck*

Hermann Keck ist externer Datenschutzbeauftragter ([www.keck-dsb.de](http://www.keck-dsb.de)).

### Tool-Download

Sie finden das Programm auf den Seiten von [www.microsoft.de](http://www.microsoft.de). Verwenden Sie im Suchfeld den Begriff „MSRSAT“ – ein Link in den Suchergebnissen verweist auf die Downloadseite.