ABSTRACT

In this work a web tool has been developed to detect how a company successfully implement the information security principles. The tool uses the security management principles defined in the ISO/IEC 27001:2007. The development language for the tool is PHP and data collected is stored in a database which is developed in MySQL. Open source instruments have been choosen because of their extensive support and usage.

The web tool collects data about the company and its IT infrastructure, then throughout an inventory, it explores the strong and weak sides of the company in terms of ISO27001 based information security principles. The tool then generates a report showing the status of the company with some advices and numerical indicators showing how that company successfully implements the information security principles. ISO/IEC 27001 divides all of the areas of the information security management into eleven sub-topics which are called as "security areas". The current test tool produces ISO/IEC 27001 compatible evaluation reports and gives a measure on how successful the company's implementation is.

Since the tool collects company information as well as the information security inventory results it is, as a priori, an invaluable instrument to findout the nation-wide information security practices all over the Turkey. It has a basic management interface with which a backoffice user (i.e. admin) can manage the system. The inventory questions and answers and security main categories can be modified throughout a web interface. Additionally, the stored inventories and company information can be listed and searched a great detail.

The tool is tested through the companies which already have a security management system. The test results show that it successfully handles the security and gives correct results. The web tool then applied to 22 companies from different sectors and data were collected and presented.

Keywords – *Information Security, Information Security Management System, ISO 27001*

ÖZET

Bu çalışmada, kurumların bilgi güvenliğini hangi başarılılıkta uyguladıklarını saptamak için, ISO/IEC 27001:2007 Bilgi Güvenliği Yönetim Sistemi prensiplerinin kullanıldığı web tabanlı bir test aracı geliştirilmiştir. Bu test aracı, kurumlardaki bilgi güvenliği altyapısının zaman içindeki durumlarının izlenmesi amacıylada kullanılabilir. Test aracı, popüler bir açık kaynak programlama dili olan PHP ile geliştirilmiş; veri tabanı yönetim sistemi olarak ise yine açık kaynak mimarisine sahip MySQL kullanılmıştır.

Web tabanlı olarak hazırlanan çevrim içi (online) anket şeklindeki bir envanter sistemi yardımıyla toplanan bilgiler ISO/IEC 27001 ölçütleri çerçevesinde değerlendirilerek, envanteri dolduran kurumun/şirketin (hem kurumsal, hem de her bir çalışanı bazında bireysel) bilgi güvenliği altyapısı ile ilgili çıkarımlarda bulunulmuştur. Ayrıca, sektörel bazda istatistiksel çıkarımlar da yapılarak, ülkemizdeki durumun kendi içinde ve dünyadaki diğer örnekleriyle karşılaştırılması hedeflenmiştir.

Çalışma, "Bilgi Güvenliği Yönetim Sistemi"nin kurum içindeki süreçlere katkısını da ortaya çıkartmaktadır. Çalışmanın son ürünü, Bilgi Güvenliği Yönetim Sistemi altyapısını değerlendirip, raporlayan bir test aracıdır (yazılım sistemi). Bu sistem, aynı zamanda, kendi içinde temel bir yönetim modülüne de sahiptir. Böylece, envanter soruları, yorumlar, bilgi güvenliği temel alanları gibi unsurlar kolayca değiştirilebilir ve yenileri eklenebilir. Envanteri dolduran firmalarla ilgili tüm bilgiler ve envanter yanıtları tüm detayları ile raporlanAbilir.

Bu araç, bilgi güvenliği yönetim sistemini oluşturmuş firmalarla test edilmiş ve güvenilirliği kanıtlanmıştır. Daha sonra, farklı sektörlerden 22 firmaya uygulanmış ve elde edilen sonuçlar listelenmiştir.

Anahtar Kelimeler – *Bilgi Güvenliği, Bilgi Güvenliği Yönetim Sistemi, ISO 27001*