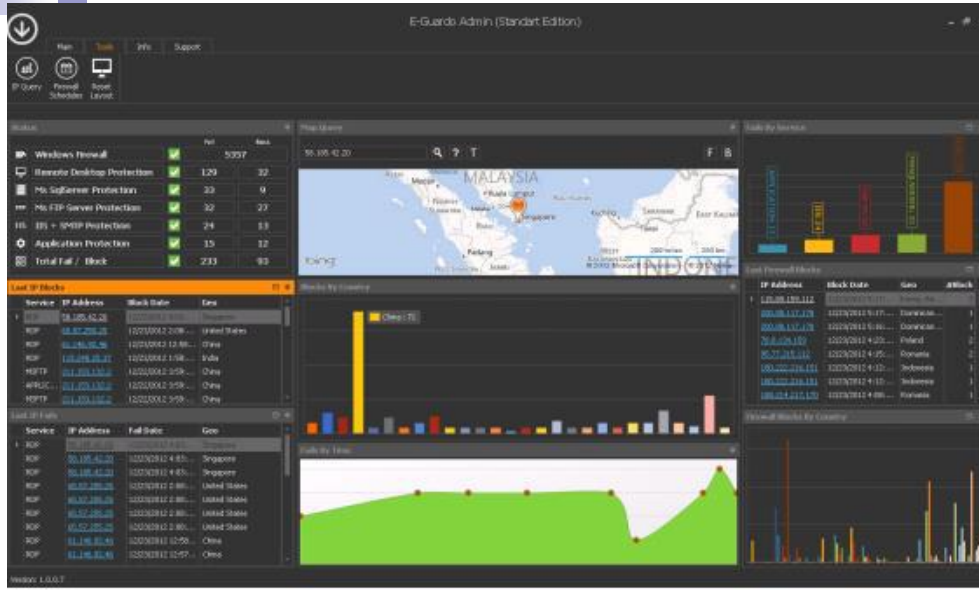


# ENTEĞRE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYUM ARACI

- Daha önceden gerçekleřtirdiĐimiz "Yapay Zekâ Temelli Bilgi GüvenliĐi Yönetimi Sistemi" yazılımımıza Milli bir saldırı/tehdit algılama ve servis güvenliĐi yazılımını entegre edilmiř aĐ üzerindeki bilgi varlıklarının zafiyetlerini tehdit eden açıklıkların otomatik olarak tespit edilmesi ve bu açıklıkların Bilgi GüvenliĐi Yönetim Sistemi dahilindeki bilgi tabanıyla karşılařtırılarak, yarattıkları risklerin ortaya konması, risklerin yönetilmesi ve azaltılması ve açıklıkların asgariye indirilmesi veya ortadan kaldırılması sağlanmıřtır.



- E-Guardo ağ üzerinde çalışan birçok servisin güvenliğini sağlamak amacıyla geliştirilmiş bir güvenlik ve saldırı algılama yazılımıdır. ABGYS ile entegre edilen yazılımın tespit ettiği saldırı türleri gruplanarak ABGYS'ne aktarılmaktadır. ABGYS tarafında dinamik olarak gelen tehditler varlık kategorileri ile eşleştirilmekte ve ABGYS dahilinde varlıkların risk analizi aşamasında tek tek değerlendirilmektedir. Böylece varsayılan risklerin yanında dinamik olarak tespit edilen risklerin de analizi yapılmakta ve bu riskleri azaltmak amacıyla tedbirler alınabilmektedir.

## ISO/IEC 27001 AKILLI BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ(ABGYS)



CYMSOFT Bilişim Teknolojileri



Son Giriş Tarihiniz : 04.01.2017 - 11:40:43 [ Administrator ]

Anasayfa Genel Ayarlar Yönetim Mevcut Durum Analizci Risk Analizci Raporcu Korumacı Uyum İzleyici İç Denetim Güvenli Çıkış

## SALDIRI ve VARLIK GRUPLANDIR

TEHDİT TÜRÜ	SALDIRI YAPILAN VARLIK	DURUM	
HEURISTIC	FIREWALL	YENİ	Tehditlere Ekle
MSSQLSERVER	MSSQL\$CRMSQL	YENİ	Tehditlere Ekle
RDP	Microsoft-Windows-Security-Auditing	YENİ	Tehditlere Ekle
IIS	URLScan	YENİ	Tehditlere Ekle
ABGYS	FIREWALL	Tehdit tablosuna kaydedilmiştir.	Tehditlere Ekle
ABGYS	FIREWALL	YENİ	Tehditlere Ekle

AKILLI BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ(ABGYS)  
CYMSOFT Bilişim Teknolojileri

- E-Guardo'nun tespit ettiği saldırı türleri gruplanarak ABGYS'ne aktarılmaktadır.

**CYMSOFT** BİLİŞİM TEKNOLOJİLERİ **CYMSOFT Bilişim Teknolojileri** ?

Son Giriş Tarihiniz : 08.01.2017 - 15:08:41 [ Administrator ]

Anasayfa Genel Ayarlar Yönetim Mevcut Durum Analizci Risk Analizci Raporcu Korumacı Uyum İzleyici İç Denetim Güvenli Çıkış

### Kategori, Zafiyet ve Tehdit İlişkilendirme

DİL :  ↻

VARLIK KATEGORİLERİ	Zafiyetler	Tehditler
<ul style="list-style-type: none"> <li>Bilgi Varlıkları                             <ul style="list-style-type: none"> <li>Kağıt doküman</li> <li>Elektronik doküman</li> <li>Elektronik veri</li> </ul> </li> <li>Yazılım Varlıkları                             <ul style="list-style-type: none"> <li>Uygulama yazılımları</li> <li>İşletim sistemi</li> <li>Kaynak kodları</li> <li>Ticari yazılımlar</li> <li>Sistem yazılımları</li> </ul> </li> <li>Donanım Varlıkları                             <ul style="list-style-type: none"> <li><b>Sunucu</b></li> <li>Depolama ünitesi</li> <li>Taşınabilir bilgisayar, PDA</li> <li>Network ünitesi</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Korumasız iletişim hatları</li> <li>Korumasız parola tabloları</li> <li>Korumasız saklama koşulları</li> <li>Kötü kullanıma açık olma</li> <li>Kullanıcı tanımlama ve silme için resmi prosedür eksikliği</li> <li>Kullanıcı tanımlama ve yetkilendirme eksikliği</li> <li><input checked="" type="checkbox"/> Kullanıma açık gereksiz servisler</li> <li>Kurum dışına çıkanlar varlıkların kontrol eksikliği</li> <li>Mekanik hasarlara açık olma</li> <li>Mesajlaşma ve iletişim ortamının doğru kullanımı için politika eksikliği</li> <li>Mobil cihaz kullanımı resmi prosesinin eksikliği</li> <li>Olgunlaşmamış veya yeni yazılım</li> </ul>	<ul style="list-style-type: none"> <li>Mesajların yanlış yönlendirilmesi (misrouting)</li> <li>Mesajların yeniden yönlendirilmesi (rerouting)</li> <li>Meteorolojik olgular</li> <li>Personelin erişilebilirliğinin ihlali</li> <li>Personelin görünüm ve davranışlarındaki uygunsuzluk</li> <li><input checked="" type="checkbox"/> RDP (E)</li> <li>Sabotaj</li> <li>Sahte veya kopyalanmış yazılımın kullanımı</li> <li>Sektör içerisinde zayıf imaj</li> <li>Silinme</li> <li>Su baskını</li> <li>Tahrifat veya sahtekarlık</li> <li>Tanınmama (repudiation)</li> <li>Tesisin kötü bir görünüme sahip olması</li> <li>Toz ve ucusan parçacıklar</li> </ul>

- ABGYS tarafında dinamik olarak gelen tehditler varlık kategorileri ile eşleştirilmektedir.

## Kontrol Tehdit

DİL : Türkçe

- Kullanılmaz hale gelme
- Kullanım hatası
- Kurcalanma
- Lisanssız kullanım
- Malzeme veya ortamın imha olması
- Mesajların yanlış yönlendirilmesi (misrouting)
- Mesajların yeniden yönlendirilmesi (rerouting)
- Meteorolojik olgular
- Personelin erişilebilirliğinin ihlali
- Personelin görünüm ve davranışlarındaki uygunsuzluk
- RDP (E)
- Sabotaj
- Sahte veya kopyalanmış yazılımın kullanımı
- Sektör içerisinde zayıf imaj
- Silinme
- Su baskını
- Tahrifat veya sahtekarlık
- ...

- A.9.1 Erişim kontrolünün iş gereklilikleri
  - A.9.1.1 Erişim kontrol politikası
  - A.9.1.2 Ağlara ve ağ hizmetlerine erişim
- A.9.2 Kullanıcı erişim yönetimi
  - A.9.2.1 Kullanıcı kaydetme ve kayıt silme
  - A.9.2.2 Kullanıcı erişimine izin verme
  - A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
  - A.9.2.4 Kullanıcılara ait gizli kimlik doğrulama
  - A.9.2.5 Kullanıcı erişim haklarının gözden geçirme
  - A.9.2.6 Erişim haklarının kaldırılması veya düzeltilmesi
- A.9.3 Kullanıcı sorumlulukları
  - A.9.3.1 Gizli kimlik doğrulama bilgisinin kullanılması
- A.9.4 Sistem ve uygulama erişim kontrolü
  - A.9.4.1 Bilgiye erişimin kısıtlanması
  - A.9.4.2 Güvenli oturum açma prosedürleri
  - A.9.4.3 Parola yönetim sistemi
  - A.9.4.4 Ayrıcalıklı destek programlarının kullanılması

KAYDET

- Dinamik tehditlerin bertaraf edilmesi için yapılması gerekenler, ilgili kontrol maddeleriyle eşleştirme ile sağlanmaktadır.

RDP (E) KAPAT

**A.9.1.1 Erişim kontrol politikası :** Bir erişim kontrol politikası, iş ve bilgi güvenliği şartları temelinde oluşturulmalı, yazılı hale getirilmeli ve gözden geçirilmelidir.

- İş güvenliğinin gerektirdiği, dokümente edilmiş ve yönetim tarafından gözden geçirilmiş bir erişim kontrol politikası bulunmalıdır.
- Kuruluş içerisinde ortak iş rollerine göre standart kullanıcı erişim profilleri bulunmalıdır.
- Erişim kontrolleri uygulanırken ticari uygulamaların gerektirdiği ayrı güvenlik ihtiyaçları göz önüne alınmalıdır.

**A.9.1.2 Ağlara ve ağ hizmetlerine erişim :** Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir.

- Kullanıcılar network kolaylıklarından kendilerine verilen yetkilerine göre faydalanabilmelidirler.
- Network yönetim kontrolleri ve network bağlantıları ile hizmetleri korumak için yönetim tarafından onaylanan bir prosedür bulunmalıdır.

**A.9.2.2 Kullanıcı erişimine izin verme :** Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi uygulanmalıdır.

- Tüm kullanıcılar şahsi kullanımları için kendine ait tek bir kullanıcı tanımına sahip olmalıdır.
- Kullanıcının kimliğini doğrulamak için uygun bir doğrulama tekniği seçilmelidir.
- Teknik destek personeli, operatörler, ağ yöneticileri, sistem programcıları ve veri tabanı yöneticileri dâhil her tür kullanıcıya kontroller uygulanmalıdır.
- Kullanıcı tanımları sorumlu personelin faaliyetlerini izlemek için kullanılmalıdır.
- Her zamanki (düzenli-rutin) kullanıcı faaliyetleri ayrıcalıklı hesaplar üzerinden yapılmamalıdır.
- İstisnai durumlarda açık bir iş çıkarı söz konusu olduğunda belli bir iş veya kullanıcı grubuna bir kullanıcı tanımının paylaşımlı kullanımı tahsis edilebilmeli ancak bu durum yönetim tarafından dokümente edilmelidir.
- Kullanıcıların faaliyetlerinin izlenmesinin gerekli olmadığı durumlarda (sadece okuma erişimi gibi) jenerik kullanıcı tanımları kullanılabilir.
- Kuvvetli yetkilendirme ve kimlik doğrulamasının gerektiği durumlarda sadece parola ile yetinilmeyip şifreleme, akıllı kartlar, tokenlar ve

- Dinamik tehditlerin bertaraf edilmesi için yapılması gerekenlerin, otomatik olarak kullanıcıya önerilmesi sağlanır.

# ENTEĞRE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYUM ARACI