Siber Güvenlik Hizmetleri
Kataloğu

TÜRKSAT

Güvenli kurumlar, sistematik yapılar!

Yetkinliklerimiz

TÜRK STANDARDLARI ENSTİTÜSÜ
BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI

SIZMA TESTİ HİZMETİ VEREN FİRMA
YETERLİLİK BELGESİ

Belge No : TSE-STF-004/TSE-PTC-004

Firma Adı	: TÜRKSAT UYDU HABERLEŞME KABLO TV VE İŞLETME A.Ş.
Firma Yetkinlik Seviyesi	: A
Sızma Testi Kapsamı	: Ağ ve Sistem Altyapısı Web Uygulamaları ve Veritabanları
Belge Veriliş Tarihi	: 23/07/2015
Belge Geçerlilik Tarihi	: 22/07/2018

Bilişim Teknolojileri Belgelendirme Müdürü
Ayşegül İBRİŞİM

Tarih : 31 / 07 / 2015

Necatibey Cad. No: 112 06100 Bakanlıklar / ANKARA
Tel: 0 (312) 416 62 00 Faks: 0 (312) 416 66 11

Information Security Management System ISO 27001 Certified

LEAD AUDITOR ISO 27001 Information Security Management System

IRCA CERTIFIED BCMS AUDITOR

C|EH™ Certified Ethical Hacker

Microsoft CERTIFIED Solutions Expert

CISCO CERTIFIED CCNP

İhtiyacınız olan adımları planlayın!

Bilgi Güvenliği Yönetim Sistemi

Temel Eğitimi
(ISO/IEC 27001:2013)

Eğitim Kodu : EGT-BGYS-01

Eğitim Süresi : 2 gün

Konular

1. Bilgi güvenliği temel tanım ve kavramlar
2. ISO/IEC 2700x standart ailesi ve destekleyici standartlar
3. ISO/IEC 27001:2005 ile ISO/IEC 27001:2013 sürümü arasındaki farklar
4. BGYS genel gereksinimler: 4. maddeden 10. maddeye kadar gözden geçirme
5. Kapsam belirleme
6. Varlık envanteri çıkarma
7. Risk yönetimi (risk metodolojileri, risk belirleme, analiz ve işleme)
8. BGYS dokümantasyonu hazırlama (politika ve prosedürler vb.)
9. Kayıt üretme ve tutma
10. Ek A kontrolleri özet
11. Uygulanabilirlik bildirgesi hazırlama
12. Etkinlik ölçümü ve iyileştirme
13. İç tetkikler (planlama, uygulama, rapor yazma)
14. Düzeltici faaliyetler
15. Yönetimin gözden geçirmesi
16. Dış tetkik ve belgelendirme süreci
17. Şartname hazırlama ve dikkat edilmesi gereken noktalar

Riskleri doğru analiz hayat kurtarır!

Bilgi Güvenliği Yönetim Sistemi

Uygulama Eğitimi
(ISO/IEC 27001:2013)

Eğitim Kodu : EGT-BGYS-02

Eğitim Süresi : 2 gün

Konular

1. ISO/IEC 2700x standart ailesi ve destekleyici standartlar
2. ISO/IEC 27001:2005 ile ISO/IEC 27001:2013 sürümü arasındaki farklar
3. BGYS genel gereksinimler: 4. maddeden 10. maddeye kadar gözden geçirme
4. Kapsam belirleme uygulaması
5. Varlık envanteri çıkarma uygulaması
6. Risk yönetimi uygulaması (risk metodolojileri, risk belirleme, analiz ve işleme)
7. BGYS dokümantasyonu hazırlama uygulaması (politika ve prosedürler vb.)
8. Ek A kontrol seçimi uygulaması
9. Uygulanabilirlik bildirgesi hazırlama uygulaması
10. Etkinlik ölçümü ve iyileştirme uygulaması
11. İç tetkik (planlama, uygulama, rapor yazma) uygulaması
12. Düzeltici faaliyet uygulaması

Olası tehlikeleri görün!

Bilgi Güvenliği Yönetim Sistemi

Kurulum ve Uygulama Danışmanlığı (ISO/IEC 27001:2013)

Danışmanlık Kodu : DNS-BGYS-01

Danışmanlık Süresi : Kurum ölçeğine göre hesaplanır. Tipik olarak 6 ay ila 18 ay arasında sürebilir.

Konular

1. ISO/IEC 27001:2013 temel ve uygulama eğitimlerinin verilmesi
2. Kapsam belirleme danışmanlığı
3. Risk yönetimi (risk metodolojisi belirleme, risk belirleme, analiz ve işleme) danışmanlığı
4. BGYS taslak dokümantasyonu temini ve dokümantasyon hazırlama danışmanlığı
5. Ek A kontrollerinin seçimi ve uygulanması danışmanlığı
6. Uygulanabilirlik bildirgesi hazırlama danışmanlığı
7. İç tetkik uygulaması danışmanlığı (planlama, uygulama, rapor yazma)
8. Güvenlik ürün ve hizmet seçimi danışmanlığı
9. İsteğe bağlı olarak diğer hizmetler (uygulama ve sistem / ağ güvenliği testleri, kaynak kod analizi vb. güvenlik hizmetleri)

Bilgi Güvenliği Farkındalık Eğitimi

Bu eğitim, çalışanların bilgi güvenliği farkındalıklarını arttırmaya yönelik olarak temel bilgileri, güncel tehditleri, saldırı türlerini ve bunlara karşı alınabilecek tedbirleri içerir.

Eğitim Kodu : EGT-BGF-01

Eğitim Süresi : ½ gün

Konular

1. Bilgi güvenliği kavramı
2. Bilgi güvenliğine yönelik güncel tehdit ve riskler
3. E-posta güvenliği
4. Kötücül yazılımlar ve karşı tedbirler
5. Sosyal mühendislik saldırıları ve karşı tedbirler
6. Bilgi güvenliği standartları ve uyum
7. ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi temel bilgiler
8. Güvenlik kontrolleri
9. Farkındalık oluşturma ve yöntemler
10. Farkındalık sınavı

Koordineli ve planlı olun!

Bilgi Güvenliği Yönetimi Sistemi İç Tetkikleri

Bilgi güvenliği yönetim sisteminin sağlıklı bir şekilde uygulanması ve iyileştirilmesi açısından iç tetkikler önem arz etmektedir. İç tetkiklerin faydalı olması ise, iç tetkik tecrübesi olan kişilerin koordinasyonunun planlı ve programlı bir şekilde yapılmasına bağlıdır.

İç Tetkik Eğitimi

Bu eğitim, iç tetkiklerin planlanmasına, tetkik ekibinin oluşturulmasına ve iç tetkiklerde dikkat edilmesi gereken noktalara ait bilgiyi içerir.

Eğitim Kodu : EGT-BGYS-03

Eğitim Süresi : 2 gün

Konular

1. ISO/IEC 2700x standart ailesi ve destekleyici standartlar
2. ISO/IEC 27001:2005 ile ISO/IEC 27001:2013 sürümü arasındaki farklar
3. BGYS genel gereksinimler: 4. maddeden 10. maddeye kadar gözden geçirme
4. Ek A kontrolleri
5. İç tetkikçi özellikleri
6. İç tetkik ekibi oluşturma
7. İç tetkik planlama
8. İç tetkik uygulaması
9. İç tetkik raporu yazma
10. Düzeltici faaliyetler ve takibi
11. Risk yönetimi ve iç tetkikte dikkat edilecek noktalar
12. BGYS dokümantasyonu ve iç tetkikte dikkat edilecek noktalar
13. Kayıtların tetkiki


Zafiyetlerinizi öngürün!

Sızma
(Penetrasyon) Testi Hizmeti

Sızma testi hizmeti, kurumsal ağınızda kapsamı belirlenen ağ / sistem ve uygulama bileşenlerinde bulunan güvenlik zafiyetlerinin belirlenmesi, analiz edilmesi ve raporlanması hizmetidir.

Sızma Testi Metodolojisi

Kurum dışından veya içinden erişilebilen bilişim varlıkları, ağ ve servislerde bulunan zafiyetler tespit edilir. Tespit edilen zafiyetlerden faydalanılarak kuruma sızma testi gerçekleştirilmektedir.

Kazanımlar

Bu hizmet, saldırganlar güvenlik zafiyetlerinizden faydalanarak kurumunuza sızmadan önce, güvenlik açıklarınızı görmenizi sağlayacaktır. Bilişim varlıklarınızın güvenlik durumunu saldırganların bakış açısıyla görmenizi ve olası saldırılarak karşı daha hazırlıklı olmanızı sağlayacaktır.

Çıktılar

Kapsamlı rapor içeriği ile bilişim varlıklarınızın zayıf yönlerini analiz edebileceğiniz, uluslararası kabul görmüş puanlama sistemi ve görsel çözüm önerileri ile zafiyetleri kolaylıkla ortadan kaldırmanızı sağlayacak bir rapor hazırlanmaktadır. Zafiyetin saldırgan tarafından nasıl istismar edilebildiği, bu durumun gizlilik, bütünlük ve erişilebilirlik alanlarına etkileri raporlanmaktadır. Raporda kapsam, metodoloji, açıkların derecelendirilmesi, yönetici özeti, bulgular ve analiz, zafiyet bilgisi ile önerilerini barındıran kapsamlı bir içerik bulunmaktadır.

Riskleri kontrol altına alın!

Güvenlik Değerlendirmesi Hizmeti

Güvenlik Değerlendirmesi (Security Assessment) bilişim varlıklarının zafiyete ve tehditlere karşı detaylı bir şekilde incelenmesidir. Sızma testleri, saldırganlarca kullanılabilecek tehditleri ortaya çıkarmaya yöneliktir. Güvenlik değerlendirilmesi ise, hatalı yapılandırmaların ve toplam tehdit noktalarının tam olarak ortaya çıkarılması için sistem üzerinde detaylı bir çalışma yapılmasıdır.

Güvenlik Değerlendirmesi Metodolojisi

Güvenlik Değerlendirmesi, otomatik araçlar ile birlikte konunun uzmanları tarafından hazırlanan ve çalışma deneyimlerinden elde edilen kontrol listelerinin ele alınması ile gerçekleştirilir. Tespit edilen bulgular, Genel Zafiyet Puanlama Sistemi (CVSS) yöntemine göre raporlanır ve kurumların ilgili zayıflıklarının giderilmesi için gerekli bilgi ile birlikte sunulur.

Kazanımlar

Bilişim varlıklarında bulunan zafiyetler tespit edilir.
Tespit edilen zafiyetler ile ilgili riskler ortaya çıkarılır.
Zafiyetin giderilmesi ve risklerin azaltılması için çözüm önerileri içeren rapor hazırlanır.

Çıktılar

Genel Zafiyet Puanlama Sistemine uygun zafiyet ve çözüm önerileri raporu hazırlanır.


BT yapınızı sağlam temellere oturtun!

Güvenlik Mimarisi Danışmanlık Hizmeti

Metodoloji

Basit veya karmaşık BT altyapılarında, bilgi teknolojileri güvenliği açısından mevcut durumun analizi, olası risklerin belirlenmesi, risk değerlendirmelerinin yapılması ve sonrasında veri, uygulama ve BT altyapı (ağ ve sistem) sistemlerini kapsayacak şekilde güvenlik mimarisinin tüm süreçlerinin oluşturulması sağlanacaktır.

Aşağıdaki 5 adımda gerçekleştirilerek kuruma özel bilgi güvenliği mimarisi oluşturulacaktır:

1. Güvenlik değerlendirmelerinin yapılması
2. Hedeflenen mimarinin tasarlanması
3. Politikaların ve prosedürlerin belirlenmesi
4. Hedef tasarımların gerçekleştirilmesi
5. İlgili tasarımların mevcut sisteme entegrasyonu

Danışmanlık Kodu : DNS-GMD-01

Kazanımlar

Bilgi güvenliği mimarisinin kurulması ile kurum BT altyapısı iç ve dış tehditlere karşı korumalı ve güvenli bir altyapı özelliği kazanacaktır.

Çıktılar

5 adımlı yaklaşım sonucunda kuruma özel bilgi güvenliği mimarisi oluşturulur.

Kötü sürprizlere yer bırakmayın!

Uygulama Güvenliği Hizmetleri

Günümüzde kurumların, iş ve yönetim süreçlerini bilgisayar uygulamaları üzerinden yürütüyor olmalarından dolayı, saldırganlar, siber saldırılarını bu alana yoğunlaştırmıştır. Gartner tarafından yapılan bir analize göre, işletmelerin %80'inin, uygulamalarda bulunan zafiyet nedeniyle bir güvenlik olayı ile karşılaşacağı, NIST tarafından yapılan başka bir araştırmaya göre ise, istismar edilebilen güvenlik açıklarının %92'sinin uygulamalarda bulunduğu belirtilmiştir. Bu nedenle uygulama güvenliğinin göz ardı edilmesi mümkün değildir.

Uygulama Güvenliği Test Hizmeti Metodolojisi

Uzmanlarımız uygulamalar üzerindeki zafiyeti ve sonucunda ortaya çıkabilecek veri sızıntılarını engellemek amacıyla çeşitli kontroller gerçekleştirmektedir. Bu testler, otomatik araçlar ile kara kutu (blackbox) testleri, özel geliştirilmiş araçlar ile liste kontrolü ve mantıksal zafiyetlere karşılık elle yapılan kontrolleri içermektedir. Bu testler sonucunda uygulamaların karşı karşıya bulunduğu tehditler, güvenlik zafiyeti ve hatalı yapılandırmalar tespit edilebilmekte ve giderilmesi amacıyla detaylı raporlar sunulmaktadır.

Kazanımlar

Zafiyet, saldırganlar tarafından kötüye kullanılmadan tespit edilir ve giderilir.
Kurumsal ve hassas verinin korunması sağlanır.
Kritik uygulamalar güvenlik açısından desteklenir.

Çıktılar

Zafiyeti gidermek amacıyla çözüm üretecek detaylı raporlar hazırlanır.

Uygulama Güvenliği Eğitimi

Eğitim Kodu : EGT-UYG-01
Eğitim Süresi : 2 Gün

Konular

1. Temel Güvenlik Kavramları
2. Güvenli Yazılım Geliştirme Yaşam Döngüsü
3. En Riskli 25 Güvenlik Açığı
4. Örnek Kontrol Listesi
5. Örnek Kara Kutu (Blackbox) Test (Uygulama)
6. Örnek Kaynak Kod Analizi (Uygulama)

Derinlemesine analiz ile önlem alın!

Kaynak Kod Analizi Hizmeti

Uygulamalar üzerinde güvenlik testleri gerçekleştirilirken sadece erişilebilen arayüzler üzerinden test yapılması yeterli olmamaktadır. Gerek arayüz bağlantısı eksik olan, gerekse o an için kullanılmayan bileşenlerde güvenlik açıkları tespit edilebilmesi için kaynak kod analizi gerçekleştirilmelidir. Kaynak kod analizi, kötü niyetli yazılan ve zamanlanmış kod bileşenlerinin tespiti için de kullanılmaktadır.

Metodoloji

Alanında lider olan kaynak kod analizi araçları ve uygulamanın özelliğine göre hazırlanmış betikler ile tüm proje ve bileşenleri analiz edilmektedir. Kaynak kod paylaşımının istenmediği durumlarda analiz, kod sahibinin ortamında ve kaynak kod TÜRKSAT bilgisayarlarına aktarılmadan gerçekleştirilebilmektedir.

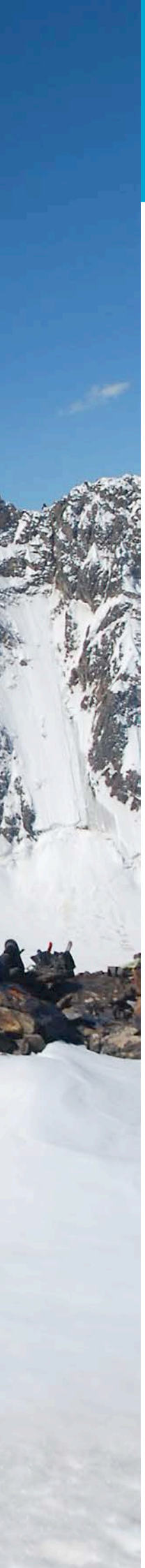
Kazanımlar

Zafiyet, saldırganlar tarafından kötüye kullanılmadan tespit edilir ve giderilir.
Kurumsal ve hassas verinin korunması sağlanır.
Kritik uygulamalar güvenlik açısından desteklenir.

Çıktılar

Zafiyeti gidermek amacıyla çözüm üretecek detaylı raporlar hazırlanır. Zafiyetin hangi uygulama bileşenlerini etkilediği raporlanır.

Kontrolü elden bırakmayın!



Merkezi Kayıt Yönetimi Sistemi Danışmanlığı

Metodoloji

Merkezi Kayıt Yönetim Sistemi (MKYS), kurum içindeki bilişim varlıklarının ürettiği logların toplanarak, tek noktadan izlenmesi, yedeklenmesi, güvenlik olaylarının tespit edilmesi için kullanılan sistemdir. Gün geçtikçe artan MKYS ürünleri, çok farklı seviyelerde özelliklere ve yeteneklere sahip olabilmektedir. Bu danışmalık ile farklı ölçeklerdeki kurumların MKYS ihtiyaçlarının belirleme, planlama, uygulama ve entegrasyon, eğitim, optimize etme ve ürün test safhalarında destek verilmektedir.

Danışmanlık Kodu : DNS-MKYS-01

Kimler İhtiyaç Duyuyor : Bünyesinde bilişim sistemlerini barındıran tüm kurumlar.

Kazanımlar

- Güvenlik olaylarının belirlenmesi sağlanır.
- Standartlar tarafındaki gereksinimler yerine getirilir.
- Kurumlar için düzenleyici kanuna (5651) uyulması sağlanır.

Çıktılar

Kurumun ihtiyaçlarını doğru karşılayan, kararlı bir MKYS sistemine yönelik kurulum, uygulama ve/veya iyileştirme raporu hazırlanır.

Ağ güvenliğinizi kontrol edin!

Aktif Ağ Cihazları Güvenliği Eğitimi

Eğitim İçeriği

Aktif Ağ Cihazları Güvenliği Eğitimi, bilgisayar ağlarında kullanılan anahtar ve yönlendiricilerine yönelik güvenlik tehditlerini, güvenlik açıklıklarının nasıl istismar edildiğini ve bu güvenlik tehditlerine karşı nasıl önlemler alınabileceğini anlatmaktadır. Ağ tarafında alınacak güvenlik önlemleri sayesinde, saldırganların hedef sistemlere erişimini kısıtlayarak ya da engelleyerek, sistem ve uygulama güvenliğinin üst düzeye çıkmasının sağlayacaktır.

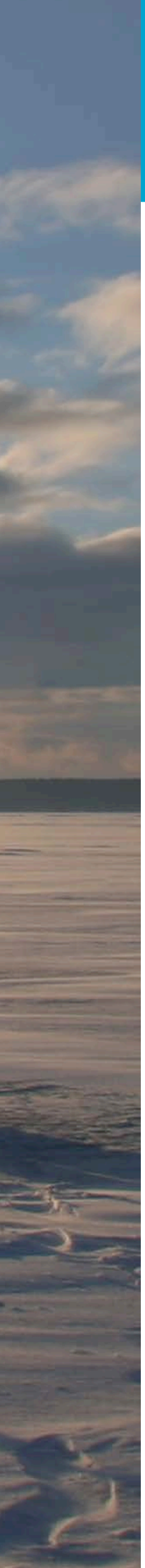
Eğitim Kodu : EGT-NET-01

Eğitim Süresi : 3 gün

Konular

1. Ağ temelleri
2. Sistemlerin güncel tutulması
3. Parola
4. Güvenli protokoller
5. AAA (Radius, Diameter, Tacacs+)
6. Gereksiz ve güvensiz servisler
7. Sistem kaynak sınırlama
8. Zaman sunucusu (NTP)
9. Erişim kontrol listeleri (ACL)
10. Uzaktan yönetim (SSH, TELNET)
11. Uzaktan yönetim (SNMP)
12. Uzaktan yönetim (HTTP)
13. Ayarlar ve sistem dosyaları
14. ICMP
15. IP
16. TCP/UDP
17. MAC
18. VLAN/DTP/VTP
19. STP
20. EIGRP/RIP
21. OSPF
22. SIEM

Dış tehditlerin oltasına gelmeyin!



Kurumsal e-Posta Güvenliği (Microsoft Exchange) Eğitimi

Eğitim İçeriği

Kurumsal firmaların büyük çoğunluğunun e-posta hizmeti olarak kullandığı Microsoft Exchange güvenliğiyle ilgili alınması gereken önlemler ve yapılandırma ayarları hakkında detaylı bilgi anlatılacaktır.

Eğitim Kodu : EGT-EXC-01
Eğitim Süresi : 2 gün

Konular

- E-Posta İletişiminde Tehditler
- Neden e-Posta Öncelikli Hedef?
  - e-Posta İstatistikleri
  - SPAM
  - Oltalama (Phishing)
  - Hedef Odaklı Oltalama (Spear Phishing)
- SMTP (Simple Mail Transfer Protocol)
- Bir e-Postanın Yolculuğu
- Bir Kurumsal e-Posta Hizmeti Microsoft Exchange
- Güvenli e-Posta Katmanları
  - Fiziksel Güvenlik
  - Sunucu Güvenliği
  - e-Posta Trafiği Güvenliği
  - Erişim Güvenliği
  - Güvenli Yetkilendirmeler
  - Kaynak Tüketimi Önlemleri
  - Kayıtların Tutulması
- E-Posta İletişiminde Personel Farkındalığını Arttırmak

"Bilgi güvenliği günümüzde kurumların işlerini sağlıklı şekilde yürütebilmeleri açısından hayati öneme sahip hâle gelmiştir. Bilgi güvenliğine yönelik saldırılar, kurumsal olarak hem maddi kayıplara, hem de itibar kaybına yol açmaktadır. Kurumsal olarak bilgi güvenliğini sağlamada en etkin yöntem, bilgi güvenliğini sistematik ve kapsamlı bir şekilde ele alarak, gerekli güvenlik tedbirlerini uygulamaktır. TÜRKSAT Siber Güvenlik Hizmetleri ile Kurumunuzun siber güvenlik ihtiyaçlarını karşılamaya yönelik hızlı ve etkin çözümler bulabileceksiniz."

T.C.
Ulaştırma Denizcilik ve
Haberleşme Bakanlığı

www.turksatbilisim.com • sgh@turksat.com.tr

TÜRKSAT