SİBER GÜVENLİK TEMELLERİ EĞİTİMİ

3 GÜN

Digital Vizyon Akademi

www.digitalvizyon.net

İçindekiler

Eğitim Hakkında 3
Neler Öğreneceksiniz? 3
Ön Koşullar 4
Kimler Katılmalı 4

Eğitim Hakkında

"Siber Güvenlik Temelleri Eğitimi", katılımcılara siber güvenlik alanında gerekli temel bilgi ve becerileri aktararak, onları bu alanda daha ileri düzeydeki çalışmalara ve uygulamalara hazırlar. Bu eğitim, siber güvenlikle ilgili temel kavramların anlaşılmasını, çeşitli tehdit türlerinin ve siber saldırı tekniklerinin tanınmasını, genel güvenlik politikalarının ve uygulamalarının anlaşılmasını hedefler.

Daha sonra, siber saldırıların nasıl gerçekleştiğini ve siber suçluların genellikle hangi teknikleri kullandığını öğrenirler. Phishing, malware, ransomware ve sosyal mühendislik gibi yaygın saldırı türleri ve bunların nasıl önlenebileceği üzerinde durulur.

Eğitimde, katılımcılar öncelikle siber güvenlik kavramını ve neden önemli olduğunu öğrenirler. Bu aşamada, veri ihlalleri, kimlik hırsızlığı, bilgisayar virüsleri ve diğer siber tehditler hakkında genel bir bakış sağlanır.

- Siber Güvenlik Anlayışı: Bu bölüm, siber güvenliğin ne olduğunu ve neden bu kadar önemli olduğunu anlamayı içerir. Katılımcılar ayrıca siber güvenliğin bir işletmenin veya organizasyonun operasyonları üzerindeki etkisini de öğrenir.
- Siber Tehditler ve Saldırı Türleri: Bu bölümde, katılımcılar çeşitli siber tehditleri ve saldırı türlerini, virüsler, truva atları, fidye yazılımları, DDoS saldırıları ve diğerleri gibi, tanımayı öğrenir.
- Siber Güvenlik Politikaları ve Prosedürler: Bu bölüm, bir organizasyonun siber güvenliğini sağlamak için hangi politika ve prosedürlerin geliştirilmesi gerektiğine dikkat çeker.
- Siber Savunma Araçları ve Teknikler: Katılımcılar, siber saldırılara karşı savunma yapmak için kullanılan çeşitli araçları ve teknikleri tanımayı öğrenir. Bu, antivirüs yazılımları, güvenlik duvarları, yama yönetimi ve daha fazlasını içerir.
- Erişim Kontrolü ve Kimlik Doğrulama: Bu bölüm, bir ağa veya sistemlere kimlerin erişebileceğini kontrol etmenin ve bu kişilerin kimliklerini doğrulamanın önemini ve nasıl yapılacağını anlatır.
- Siber Olay Yönetimi ve Yanıt: Bu bölüm, bir siber olayın nasıl tanımlanacağını, nasıl yanıt verileceğini ve olay sonrası toparlanmanın nasıl gerçekleştirileceğini anlatır.
- Siber Güvenlikte Yasal Hususlar ve Uyumluluk: Bu bölüm, siber güvenlik alanındaki yasal düzenlemeleri ve uyumluluk gerekliliklerini tanıtır.

Neler Öğreneceksiniz?

Siber güvenlik temelleri eğitiminde, şunları öğrenebilirsiniz:

- Siber güvenlik kavramları: IP adresleri, ağ güvenliği, veri şifreleme, güvenliği sağlanmış veri depolama vb.
- Siber tehditler: Virüsler, solucanlar, kötü amaçlı yazılımlar, sosyal mühendislik saldırıları vb.
- Güvenli ağ yapısı: Firewall teknolojileri, DMZ, güvenli ağ tasarımı vb.

- Veri güvenliği: Veri şifreleme teknikleri, veri yedekleme ve geri yükleme işlemleri, veri güvenliğini sağlayan yazılımlar vb.
- İşletmeler için siber güvenlik: Kurumların siber güvenliği politikaları, siber güvenliğe dair standartlar ve mevzuatlar, siber güvenliğe dair en iyi uygulamalar vb.
- Siber saldırıları önleme yöntemleri: Ağ güvenliği kontrolleri, güncel siber güvenlik yazılımları, güvenli ağ tasarımı, veri şifreleme vb.
- Siber güvenlik eğitimi ve profesyonel gelişimi: Siber güvenliğe dair en son teknolojik çözümler, siber güvenlik eğitimi ve profesyonel gelişim fırsatları vb.
- Bu eğitim, siber güvenliğe dair temel bilgileri ve becerileri kazandırmanın yanı sıra, siber güvenliği konularında daha derinlemesine bir anlayış kazandırmayı amaçlar. Aynı zamanda, siber güvenliğe dair en iyi uygulamaları ve teknolojik çözümleri tanıtmakta ve bu konuları uygulamalı olarak öğrenmek için fırsat sunmaktadır.

Ön Koşullar

Siber güvenlik eğitimine katılmak için genellikle aşağıdaki ön koşullar bulunabilir:

- Bilgisayar ve İnternet Bilgisi: Siber güvenlik eğitiminde, bilgisayar sistemleri, ağlar ve internet güvenliği gibi konuları anlamak için bilgisayar ve internet bilgisi gerekir.
- Programlama Bilgisi: Siber güvenlik eğitiminde kullanılan araçlar ve teknolojiler hakkında bilgi sahibi olmak için programlama bilgisi faydalıdır.
- İşletim Sistemi Bilgisi: Siber güvenlik eğitimi içerisinde, işletim sistemi güvenliği ve açıklıkları hakkında bilgi sahibi olmak için işletim sistemi bilgisi gerekir.
- İngilizce Bilgisi: Siber güvenlik dokümantasyonları ve materyalleri genellikle İngilizce olarak sunulur, bu nedenle iyi bir İngilizce bilgisi eğitimi tam olarak anlamanıza yardımcı olabilir.

Bu ön koşullar eğitim verilen yere ve eğitimin içeriğine göre değişebilir. Ancak, bu ön koşullar siber güvenliğe dair temel bilgileri anlamanıza yardımcı olacaktır.

Kimler Katılmalı

Siber güvenlik eğitimi, aşağıdaki kişiler için faydalı olabilir:

- IT profesyonelleri: Siber güvenlik uzmanı, sistem yöneticisi, ağ yöneticisi gibi IT profesyonelleri, siber güvenlik konularını daha iyi anlamak ve uygulamak için bu eğitimden faydalanabilir.
- Güvenlik Uzmanları: Siber güvenlik uzmanları, siber tehditleri tanımlamak, analiz etmek ve önlemler almak için gereken bilgi ve becerileri geliştirmek için bu eğitimi tercih edebilir.
- Geliştiriciler: Yazılım ve web geliştiricileri, uygulamalarının güvenliğini sağlamak için gereken bilgi ve becerileri öğrenmek için bu eğitimi tercih edebilir.
- İşletmeler ve Kurumlar: İşletmeler ve kurumlar, siber tehditlere karşı kendilerini ve verilerini korumanın yollarını öğrenmek için bu eğitimi tercih edebilir.

- Cybersecurity Meraklıları: Siber güvenlik konularına ilgi duyan ve bu alanda kariyer yapmak isteyen kişiler de bu eğitimi tercih edebilir.

Bu eğitim, siber güvenliğe ilgi duyan ve bu alanda beceri geliştirmek isteyen herkes için faydalı olabilir. Ancak, eğitimin içeriği ve zorluk seviyesi kişinin bilgi seviyesine göre değişebilir.