Ders Planı

2023-1-SK01-KA220-SCH-00015112

Başlık	Güvenlik ve Dijital Araçlar	
Blok Başlığı	**Siber Koruyucular: Dijital Araçlar Aracılığıyla Güvenliği Keşfetmek**	
Yaş kategorisi 9-16	**Süre (dk)** 100 dk	**Ders saati sayısı** 3

Öğrenci odaklı eğitim hedefleri (içerik ve performans standartları)

Ana Hedef: Siber Güvenliğin Önemini Anlamak. Öğrenciler, farklı dijital güvenlik tehditleri ve teknolojinin bilgi ve verileri korumak için nasıl kullanılabileceği hakkında bilgi edinecekler. 3D World, siber güvenlik senaryolarını simüle etmek için kullanılacak ve öğrenciler, tercihen ekip çalışması yaparak, ekip çalışmasını ve yenilikçi problem çözme becerilerini geliştirerek bu senaryoları çözebilecekler.

Didaktik materyaller ve didaktik teknikler

- 3D Dünya ortamının barındırılacağı internete veya yerel ağa erişimi olan bilgisayarlar.

Referanslar/Kaynaklar (videolar, metodolojiler)

Motivasyonel aşama

Süre (dk): 10 dakika

Amaç, dijital güvenlik hakkında bir giriş yapmak ve öğrencilerin çevrimiçi bilgileri korumanın önemi hakkında düşünmelerini sağlamaktır. Bu, bir Labirenti andıran Sanal Dünya'da bir etkinlikle gerçekleştirilebilir.

Öğrenciler, başında "Siber Dünya Labirenti" yazan büyük bir labirente ulaşacaklar. Labirentte, kimlik avı e-postaları, kötü amaçlı yazılımlar veya parola kırma gibi yaygın güvenlik tehditlerini temsil eden farklı engellerle karşılaşacaklar. Her engel için, bu dijital tehditlerden kaçınmanın veya bunları azaltmanın yollarını belirlemelerini gerektiren bulmacalar ve sınavlar gibi zorluklarla karşılaşacaklar. Bu

zorlukları çözmek, öğrencilerin labirentin çıkışını bulmalarını sağlayacak.

Keşif aşaması

Süre (dk): 20 dk

Amaç, öğrencileri siber güvenlik araçlarının nasıl çalıştığını keşfetmeye teşvik ederek, etkileşimli öğrenme yoluyla dijital güvenliğin temel ilkelerini keşfetmelerini sağlamaktır. Bu aşamada önerilen etkinliğin adı "Sanal Güvenlik Sisteminizi Oluşturmak"tır. Öğrenciler, kurgusal bir şirket veya kuruluş için sanal bir güvenlik sistemi tasarlamak, olası güvenlik tehditlerini ele almak ve çözümler önermek için ekipler halinde çalışmalıdır.

Öğrenciler, virüsler, kimlik avı saldırıları ve veri ihlalleri gibi farklı siber güvenlik tehditlerini inceleyeceklerdir. Ayrıca güvenlik duvarları, şifreleme ve çok faktörlü kimlik doğrulama gibi temel güvenlik araçlarını da araştıracaklardır. Sanal dünya platformunu kullanarak öğrenciler, güvenli bir ofis ortamının veya veri merkezinin dijital bir temsilini oluşturacaklardır. Parola korumalı giriş, şifreli veri kasaları ve güvenlik duvarları gibi unsurları dahil edeceklerdir. Takımlar, sanal dünyalarında olası güvenlik ihlallerini (örneğin, veri çalmaya çalışan bilgisayar korsanları) simüle edecek ve güvenlik sistemlerinin kuruluşu nasıl koruduğunu göstereceklerdir. Tasarımı tamamladıktan sonra, her takım dahil etmeyi seçtikleri güvenlik özelliklerini ve belirli tehditleri nasıl ele aldıklarını tartışacaktır.

Planlanan faaliyete dahil edilmesi gereken bazı temel unsurlar şunlardır:

Virüslerin, kötü amaçlı yazılımların ve diğer siber tehditlerin teknik düzeyde nasıl çalıştığını anlamak.

Şifreleme, güvenlik duvarı ve parola koruması gibi güvenlik araçlarının uygulanması.

Gerçek dünya sorunlarını çözmek için işlevsel, sanal bir güvenlik sistemi tasarlamak.

Şifreleme anahtarlarının hesaplanması, veri iletim hızlarının belirlenmesi veya bir parolanın ne kadar güvenli olduğunun belirlenmesi.

Güvenlik sistemi için ilgi çekici, kullanıcı dostu bir arayüz oluşturmak.

Fiksasyon fazı (pekiştirme ve derinleşme)

Süre (dk): 30dk

Önerilen etkinliğin başlığı "Siber Güvenlik Mücadelesi: Geleceği Güvence Altına Almak"

Amaç, öğrencilere gerçek dünyadan bir siber güvenlik sorunu sunulması ve kurgusal bir organizasyonu veya grubu siber saldırılardan korumak için dijital bir çözüm tasarlamaları görevi verilmesidir.

Üç alternatif senaryo mevcut olacak:

Akıllı hoparlörler, kameralar ve ev aletleri gibi internet bağlantılı cihazlarla (IoT) donatılmış akıllı bir evi

korumak için bir güvenlik sistemi tasarlayın. Çözüm, yetkisiz erişim ve veri ihlalleri gibi tehditleri ele almalıdır.

Öğrenci verilerini korumaya, bilgisayar korsanlığını önlemeye ve öğretmenler, öğrenciler ve veliler arasında güvenli iletişimi sağlamaya odaklanan bir okul ağı için siber güvenlik planı geliştirin.

Hassas hasta verilerini işleyen bir sağlık kuruluşu için siber güvenlik çözümü oluşturun. Sistem, gizliliği korurken aynı zamanda bilgisayar korsanlığına, yetkisiz erişime ve veri ihlallerine karşı koruma sağlamalıdır.

Öğrencilerin izleyeceği adımlar şu şekildedir:

1. **Öğrenciler bir senaryo seçer ve söz konusu senaryoda yer alan belirli siber güvenlik risklerini (örneğin, bilgisayar korsanlığı, veri hırsızlığı, fidye yazılımı) belirler.**
2. **Ekipler, hangi siber güvenlik araçlarının (örneğin şifreleme, güvenlik duvarları, kimlik doğrulama sistemleri) uygulanabileceğini değerlendirerek çözümler üzerinde beyin fırtınası yaparlar. Sanal dünya platformunda bir prototip tasarlayacaklardır.**
3. **Öğrenciler sanal dünyayı kullanarak bir siber saldırı senaryosunu (örneğin, bir bilgisayar korsanının bir sisteme girmeye çalışması) simüle edecekler. Takımlar, güvenlik çözümlerinin kuruluşu saldırıdan nasıl koruduğunu gösterecekler.**
4. **Ekipler, dijital güvenlik prototiplerini sınıfa sunarak nasıl çalıştığını ve senaryonun oluşturduğu tehditleri nasıl ele aldığını açıklar. Öğretmen ve akranlarından gelen geri bildirimler, çözümlerini geliştirmelerine yardımcı olabilir.**

Öğrenci Değerlendirmesi

Sanal labirente katılım ve çıkış yolunu bulma.

Sanal dünyada tasarlanan dijital güvenlik sisteminin yaratıcılığı ve işlevselliği.

Dijital araçları kullanarak güvenlik çözümlerinin belirli tehditlere nasıl yanıt verdiğini açıklayabilme ve sunum yapabilme becerisi.

Ekler:

Bu proje, Avrupa Komisyonu'nun desteğiyle yürütülmüştür. Avrupa Komisyonu'nun bu yayının hazırlanmasına verdiği destek, yalnızca yazarların görüşlerini yansıtan içeriğin onaylandığı anlamına gelmez ve Ajans ve Ulusal Komisyon, burada yer alan bilgilerin herhangi bir şekilde kullanılmasından sorumlu tutulamaz.