Task 1: What is the role of the playbook concept in incident response? Why do we need it?

Bir playbook, her oyuncunun nerede ne zaman ne yapması gerektiği ve ne söyleyeceğinin belirtildiği bir tiyatro oyununun senaryosu gibi düşünülebilir. Siber güvenlikte bir incident response için oluşturulan playbookta aynı amaca hizmet eder.

Playbooklar, belirli bir olay türüne karşı tepkiyi standartlaştırarak, organizasyonların belirli olay türlerine hazırlanmak, yanıtlamak ve onlardan kurtulmak için alması gereken belirli adımları içeren prosedürleri sağlar.

Playbooklar birkaç açıdan kritik olarak değerlendirilebilir. İlk olarak, düzenli ve yapılandırılmış bir yaklaşım sağlamaları nedeniyle bir ihlalin ortaya çıktığı kaos ortamında el altında bulunan bir playbook, bilinmeyen bir ortamda hareket etmek için bir pusulaya sahip olmak gibi, zorluklar içerisinde yol bulmaya yardımcı olacaktır. İkinci olarak ise bir playbook, müdahale ekiplerinin standart bir süreci takip etmesini sağlayarak kiritik adımların gözden kaçmasını veya baskı altında hata yapma riskini azaltacaktır. Ayrıca bir saldırıya müdahale planını saldırı esnasında oluşturmak yerine ekipler önceden tanımlanmış eylemleri gerçekleştirerek zaman kazanma konusunda son derece yardımcı olacak, saldırganın sistemlerde geçireceği zamanı aza indirmesi nedeniyle çok değerli olacaktır. Bunun yanında müdahale ekiplerine yeni katılan personel playbooklara başvuraral daha hızlı bilgi sahibi olabilirler, yeni personelin eğitimine katkı sağlamanın yanında organizasyonun belirli güvenlik olayları ile mücadele süreçlerini daha kolay anlayabilirler.

Playbooklar statik belgeler değildir. Tehditlerin sürekli olarak değiştiği gibi zaman içerisinde teknoloji ve süreçlerdeki değişikliklere ayak uydurmak üzere düzenli olarak güncellenmelidir.

En genelinde bir playbook, güvenlik olaylarıyla etkili ve verimli bir şekilde başa çıkmak için stratejik bir rehberdir. Potansiyel olarak kaotik ve stresli bir durumu iyi düzenlenmiş bir yanıt haline getirir, hızlı ve başarılı bir çözüm şansını artırır. Belirli bir sırayla olayların tespit edilmesi, sınırlanmasını ve giderilmesini sağlayarak organizasyonun güvenlik postürüne katkıda bulunurlar.

Task 2: Write a ransomware playbook.