Defence in Depth

Defence in depth, Türkçeye Derinlemesine savunma olarak çevrilmektedir. Adından da anlaşılacağı gibi savunma şeklinin tek bir açıdan değil de çok yönlü olarak ayrıntılı bir şekilde savunulması anlamına gelmektedir. Bunun amacı, tek bir güvenlik önleminin başarısız olma olasılığından kaynaklıdır. Savunma sayısı ve gücü arttığında bilgilerin korunması da o kadar artmış olmaktadır. Ayrıca askeri bir stratejiden faydalanılarak ortaya çıkan bu savunma taktiği, saldırganı güçlü olan tek bir savunma hattıyla yenmek yerine adım adım ilerlemesini geciktirmeyi amaçlamaktadır.

Derinlemesine savunmanın kendisine özgü bir mimarisi bulunmaktadır ve bu katmanlı güvenlik olarak da adlandırılmaktadır. Asıl amaç, saldırgan bir savunma katmanını geçerse diğer savunma katmanında takılı kalarak kontrol altına alınılmasını sağlamaktır. Temel olarak 3 kontrol noktası olduğu söylenilebilmektedir. Bunlar;

- Fiziksel kontroller
- Teknik kontroller
- İdari kontroller

şeklindedir.

Fiziksel kontroller, fiziksel olarak erişilmesini önleyen kontrol çeşididir. Özel güvenlikler, çitler veya köpekler bunlara örnek verilebilmektedir.

Teknik kontroller, özel donanım ya da yazılımlar kullanılarak sistemi koruyan güvenlik çeşididir. Disk şifreleme, kimlik doğrulama teknik kontrollere örnek olarak verilebilmektedir.

İdari kontroller, kuruluşun prosedürlerini kapsamaktadır. Uygun bir rehberliğin bulunması sonucu güvenliğe en uygun bir şekilde hareket edilmesini sağlayan kontrol çeşididir. İşe alma uygulamaları, hassas bilgileri “gizli” etiketi ile ilerletmek bunlara örnek olarak verilebilmektedir.

Bunlara ek olarak farklı güvenlik katmanlarının kullanılması da derinlemesine savunmaya katkı sağlayan önemli bir adımdır. Örneğin, ağ güvenlik çözümleri için VPN, güvenlik duvarları kullanılması; İzinsiz girişleri önlemek için IDS/IPS araçlarının kullanılması; Uç nokta güvenlik çözümleri için EDR araçlarının kullanılması; kullanıcı kimliği erişim yönetimi için çok faktörlü kimlik doğrulama kullanılması gibi birçok güvenlik öğeleri kullanılmaktadır.

Saldırganı engellemek için birçok yol bulunmaktadır. Bu yolların tek birinin kullanılması yerine birbiri ile en uyumlu olan ve birleşmeleri sonucu her yönden koruma sağlayan çözümlerin aynı anda kullanılması savunma açısından sağlıklı olandır. Bu sayede derinlemesine savunma taktiği saldırganları büyük ölçüde engelleyen bir strateji haline gelmektedir.

Zeynep YILDIZ