Olay raporu analizi

Özet	2 saat süren bu saldırıda güvenlik duvarında bulunan bir güvenlik açığından dolayı (Güvenlik duvarının doğru yapılandırılmamış olması) Ddos saldırısına kuruluşun ağ hizmetleri saldırı altında kalmıştır. . Ekip, saldırıyı engelleyerek ve kritik olmayan tüm ağ hizmetlerini durdurarak yanıt verdi, böylece kritik ağ hizmetleri geri yüklenebildi.
Tanımlamak	Kötü niyetli bir aktör veya aktörler, bir ICMP sel saldırısı ile şirketi hedef aldı. Tüm dahili ağ etkilendi. Tüm kritik ağ kaynaklarının güvence altına alınması ve çalışır duruma getirilmesi gerekiyordu.
Korumak	**Güvenlik duvarının kuralların ayarlanması ve güncellenmesi yapıldı.** **Kaynak ip adresini kontrol edici bir sistemin oluşturuldu.** **Ağ izleme yazılımları kuruldu. Örneğin Wireshark, Solarwinds benzeri. Bunlar monitörize edildi. aktif olarak takip altına alındı.** **Ayrıca IDS yada IPS sistemi kuruldu.**
Algılamak	Siber güvenlik ekibi, gelen ICMP paketlerinde sahte IP adreslerini kontrol etmek için güvenlik duvarında kaynak IP adresi doğrulamasını yapılandırdı ve anormal trafik modellerini tespit etmek için ağ izleme yazılımı uyguladı.

Yanıt	Gelecekte tekrardan böyle bir saldırı olması durumunda ilk olarak gelen paketlerin analizi yapılmalıdır bunun içinde wireshark benzeri bir ağ izleyici hazırda olmalıdır. Ardından bu saldırıya bir cevap verdiğimizi örnek alırsak paketlerin hangi güvenlik duvarı boşluğundan geldiğini tespit edip müdahale etmeliyiz burda işimizi kolaylaştıması için aktif olarak SIEM araçlarından yararlanabiliriz. ayrıca tüm olayları üst yönetime ve varsa ilgili yasal makamlara bildirilmelidir.
İyileşmek	İyileştirme olarak şu tavsiyeleri uygulayabiliriz ICMP trafiğini filtrelemek için bir IDS/IPS sistemi kurulabilir. Ağ izleme yazılımları aktif olarak kullanılabilir. Özellikle güvenlik duvarları ayarları özenerek yapılabilir.

Yansımalar/Notlar: