Küçük işletmelere web tasarım hizmetleri, grafik tasarım ve sosyal medya pazarlama çözümleri sunan bir multimedya şirketinde çalışan bir siber güvenlik analistisiniz. Kuruluşunuz yakın zamanda, çözülene kadar iki saat boyunca dahili ağı tehlikeye atan bir DDoS saldırısı yaşadı.

Saldırı sırasında, kuruluşunuzun ağ hizmetleri gelen bir ICMP paketi seli nedeniyle aniden yanıt vermeyi bıraktı. Normal dahili ağ trafiği hiçbir ağ kaynağına erişemedi. Olay yönetim ekibi gelen ICMP paketlerini engelleyerek, kritik olmayan tüm ağ hizmetlerini çevrimdışı bırakarak ve kritik ağ hizmetlerini geri yükleyerek yanıt verdi.

Şirketin siber güvenlik ekibi daha sonra güvenlik olayını araştırdı. Kötü niyetli bir aktörün yapılandırılmamış bir güvenlik duvarı aracılığıyla şirketin ağına bir ICMP ping seli gönderdiğini buldular. Bu güvenlik açığı, kötü niyetli saldırganın dağıtılmış hizmet reddi (DDoS) saldırısı yoluyla şirketin ağını alt üst etmesine olanak sağladı.

Bu güvenlik olayını ele almak için ağ güvenlik ekibi şunları uyguladı:

- Gelen ICMP paketlerinin hızını sınırlamak için yeni bir güvenlik duvarı kuralı
- Gelen ICMP paketlerinde sahte IP adreslerini kontrol etmek için güvenlik duvarında kaynak IP adresi doğrulaması
- Anormal trafik modellerini tespit etmek için ağ izleme yazılımı
- Şüpheli özelliklere göre bazı ICMP trafiğini filtrelemek için bir IDS/IPS sistemi

Siber güvenlik analisti olarak, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Siber Güvenlik Çerçevesi'ni (CSF) izleyerek şirketinizin ağ güvenliğini iyileştirmek için bir plan oluşturmak üzere bu güvenlik olayını kullanmakla görevlendirilirsiniz.