SCOP NET

NAC+Tehdit
Analiz Platformu

360° SİBER GÜVENLİK
SCOP
SCOP NET
Kurumsal ağlara giriş kontrolü ve tehdit yönetiminde yeni bir boyut
SCOP VISION
Elasticsearch tabanlı büyük veri platformu ile benzersiz performans
SCOP MON
Gerçek zamanlı ağ ve sistem izleme
SCOP SOC
Bütünleşik ve entegre güvenlik yönetim platformu
SCOP DESK
Uçtan uca benzersiz hizmet yönetimi

NAC Çözümü Gerekliliği

Siber güvenlik, İnternet üzerinden bağlantı halindeki bir dünyanın temel taşıdır. Önümüzdeki yıllar içerisinde dünya genelinde internet kullanıcılarının, aygıtların ve verilerin sayısında yüksek miktarda artış, büyük fırsatların yanı sıra aynı derecede göz korkutucu zorlukları da beraberinde getirecektir.

Siber güvenlik, bilgi güvenliğinden operasyon güvenliğine ve bilgisayar sistemlerinin güvenliğine, ağ erişim kontrol güvenliğine (**NAC**), log ve olay yönetim güvenliğine(**SIEM**), ağ ve sistem cihazlarının takibinin yapılmasın kadar birçok farklı kavramı kapsar. Siber güvenlik aynı zamanda farklı hedef kitleleri için farklı anlamlara gelir. Bireyler açısından bu kavram güvenli hissetmek, kişisel verileri ve gizliliği korumak demektir.

Kurumlar açısından siber güvenlik, işle ilgili kritik öneme sahip bilgilerin kullanılabilir olmasını, operasyon ve bilgi güvenliği sayesinde gizli verilerin korunmasını sağlamak demektir. Siber güvenlik bireylerin, kurumların bilgi işlem hedeflerine güvenli, özel ve güvenilir bir şekilde ulaşmalarına olanak veren ortak etkinlikleri ve kaynakları ifade eder.

Bilgi teknolojilerine bağımlılık bir dizi riski de beraberinde getirmektedir. Güvenli ağlara saldırganlar çeşitli yöntemlerle saldırabilmekte, üstelik bunu anonim olarak ve gizli bir şekilde yapabilmektedir. (Bir tuş vuruşunun dünyanın çevresini dolanması yüz elli milisaniye sürer) Mobil aygıtlar hızla yaygınlaşmakta ve hatta geleneksel kişisel bilgisayarların önüne geçmektedir. Dünya çapındaki Internet kullanıcılarının sayısındaki artış nedeniyle, bu kullanıcılar yeni güvenlik açıklarına yol açabilmektedir.

Kurum ağlarının güvenli kalabilmesi için ağa bağlanan ve bağlanacak cihazların belirli kontrollere tabi tutulması gerekmektedir. Günümüzde ağa bağlanması gereken cihaz tipleri ve bağlantı şekilleri çeşitlenmektedir. Kurum personelinin kendi şahsi cihazları, kuruma gelen misafir personelin ya da kuruma desteğe gelen firma personelin bağlantı gereksinimleri ağ güvenliğini riske sokmaktadır. Bu riskleri minimuma indirgemek için Ağ Erişim Kontrol Sistemleri (**NAC**) kullanılmaktadır.

NAC Çözümünden Beklentiler Nelerdir?

İşletmelerde teknoloji kullanımı arttıkça siber saldırıların zararları da hızla artmaktadır. Mayıs 2017'de 100 ülkedeki hastaneler, şirketler ve devlet dairelerinde bulunan 57.000'den fazla bilgisayarı etkileyen büyük bir siber saldırı düzenlenmiş ve saldırıya uğrayan bilgisayarlardaki dosyalar şifrelenerek dosyaların şifrelerinin çözülmesi için kurbanlardan fidye istenmiştir. 2017 Verizon Veri İhlali Araştırma raporunda, ihlallerin %81'inde çalıntı veya zayıf şifrelerin, %51'inde ise kötü amaçlı yazılımların kullanıldığı belirtilmektedir.

Günümüzde giderek artan güvenlik tehditlerini kurum ağından uzak tutmak, kurum ağında olan cihazları ve durumlarını sürekli izleyebilmek, kurum ağına bağlanacak cihazlar için politikalar belirlemek ve bu politikalara uymayan cihazların ağa erişimlerini engelleyebilmek veya sınırlayabilmek önem arz etmektedir. Bu maksatla kurum ağına erişmek isteyen sistemlerin, belirleyeceğimiz güvenlik politikalarına uygunluğunun kontrol edilmesi, belirlediğimiz politikalara uygun cihazların erişimine izin verip, uygun olmayan cihazların erişiminin engellenmesi için Ağ Erişim Kontrol sistemi (**NAC**) kurulumu gereklidir.

ScopNET Nedir?

Yetkisiz cihazların kurumsal ağa dahil olması önemli güvenlik risklerini beraberinde getirmektedir. Bu cihazlar, kurumsal BT güvenlik korumalarına sahip olmadıklarından üzerlerinde çeşitli zararlı yazılımlar bulundurabilir. Bu zararlı yazılımlar kurumsal verilere erişebilir veya iş servislerinin kesintiye uğramasına neden olabilir.

ScopNET Neden Farklıdır?

ScopNET organizasyonların ağlarına dahil olmaya çalışan dış cihazlar için ağ katılma politikalarını uygular. Dahil olan cihazlara ajan kurulumu yapılmadan ve 802.1x bağımlılığı olmadan politika kurallarına göre cihazların ağa bağlanmalarına izin verir ya da ağa dahil olmalarını engeller. Envanter toplama özelliği sayesinde kurum bilgisayarlarının durumlarını denetler ve kullanım kurallarına uymayan kurum bilgisayarlarını kurallar dahilinde isteğe bağlı olarak engeller ya da tanımlanmış uyarılar ile BT yönetim ekiplerini bilgilendirir.

Tehdit Yönetiminde Yeni Bir Boyut;

- ScopNET sistemler üzerinde çeşitli analizler yapar.
- Gerçekleştirilen Başlıca Analizler
- Dışarıya bağlantı kuran programlar
- Cihazların birbirleri ile olan bağlantıları
- Uygulamalar tarafından yaratılan ağ trafiği
- Port tarama işlemleri
- Zayıf SNMP parolalarının tespiti, zayıf işletim sistemi parolalarının tespiti
- Kötü amaçlı yazılımların tespit edilmesi
- Kötü niyetli sistem sürücüsü analizi
- Kötü niyetli servis analizi, kötü niyetli otomatik çalışan program analizi
- Kötü niyetli zamanlanmış işlemler çalışma analizi

ScopNET Kullanımı Sonrası Kazanımlar;

- ScopNET bilgisayarlar üzerinde ajan kurulmadan çalışabilir. Diğer ürünlere göre bileşen ya da ajan kurmadan, uzaktan çalışabilen tek üründür.
- ScopNET, şifre değiştirilmesi, hesap kilitlenmesi, olay kayıtlarının silinmesi, hesap gruplarının değiştirilmesi gibi önemli güvenlik olaylarını takip edebilir, takip işlemi sırasında güvenlik açığı olduğuna karar verilen cihazların ya da hesapların sisteme erişimini engelleyebilir.
- ScopNET, ağ cihazları üzerinde doğrudan komut çalıştırılmasına olanak sağlar. Bu yapı büyük sistemlerde verimliliği artırır. SSH/Telnet/SNMP protokolünü destekleyen tüm cihazlar ile kolaylıkla entegrasyon sağlanır.
- ScopNET, ağ üzerinde herhangi bir yapısal değişiklik gerektirmeden, ağ altyapısı üzerinde birden fazla yöntem kullanarak tespit ve engelleme yapabilmektedir.
- Yerli ve Milli ürün olma avantajı ile düşük operasyonel maliyetler.
- Uygulama ve servis envanterlerinin çıkarılması,
- Microsoft WSUS durumu ve Antivirüs güncelleme durumu ve analizi
- USB kullanımı takibi, Windows AutoRun Kayıtları
- Genel WMI Envanteri, Windows Kütük Envanteri
- Hatalı Kullanıcı Girişleri, Port Taramaları
- Önemli Windows Olay Kayıtları

- Ağ Bağlantı Ayarları, Virtual Host NAT Analysis
- Dosya Analizi ve BitLocker Kullanımı tespiti
- Windows Güvenlik Merkezi Analizi
- Zayıf SNMP Şifre Analizi, zayıf Windows Şifre Analizi
- Bant genişliği Kullanımı, TCP Bağlantı Analizi
- Dinleme Portu Açan Uygulama Analizi, zamanlanmış görevler analizi
- Windows Sürücü Analizi