MARSH

Evden Çalışma için Siber Güvenlik İpuçları #MarshCyber

- Ağa, yalnızca gerektiğinde güvenli bir kanal üzerinden(VPN) uzaktan erişimi etkinlestirin.
- Mümkünse 2 kademeli kimlik doğrulamayı etkinleştirin.
- Uzak hizmetleri yalnızca güvenli protokoller yardımıyla kullanın (HTTPS).
- Uzaktan erişimi yalnızca yetkili servislerle ve ağdaki yalıtılmış bölgelere kısıtlayın.
- Uzak cihazlardaki güvenlik sistemlerini kontrol edin (örn. Antivirüs, güvenlik güncellemeleri, güvenlik yapılandırması vb.).
- Uzak aygıtların uzaktan engellenme ve sıfırlanma özelliklerini gözden geçirin.
- Tüm kişisel cihazların disk şifrelemesine sahip olduğunu ve veri sızıntısını önleme kontrollerinin mevcut olduğunu doğrulayın.
- Kritik bilgileri yedekleyin.
- Farkındalık, farkındalık ve farkındalık (ör. Kimlik avı, phishing gibi kötü amaçlar için kullanılan sistemlerin tespiti)
- Şüpheli bir olayı bildirmek için çalışanların izlemesi gereken protokolleri tanımlayın.
- Siber güvenlik izleme düzeylerini artırın. En azından aşağıdaki incelemeleri ekleyin:
  - Başarısız oturum açma denemeleri ve ardından başarılı girişimler.
  - Birden fazla IP adresinden (veya konumdan) tek bir kullanıcıyla erişim.
  - Şüpheli veya anormal ağ trafiği.
  - Olağandışı konumlardan veya ülkelerden uzaktan bağlantı.
- Şirket hizmetlerine erişmek için genel veya güvenli olmayan ağların kullanılmasını önlemek için kullanıcıları eğitin.

Evden çalışma stratejilerinin internet bağlantı kapasitelerini doldurabileceğini unutmayın. Hizmetlerin kullanılabilirliğini sağlamak için kapasitesinizi gözden geçirin ve internet bağlantılarını sürekli olarak izleyin.

MARSH & McLENNAN COMPANIES