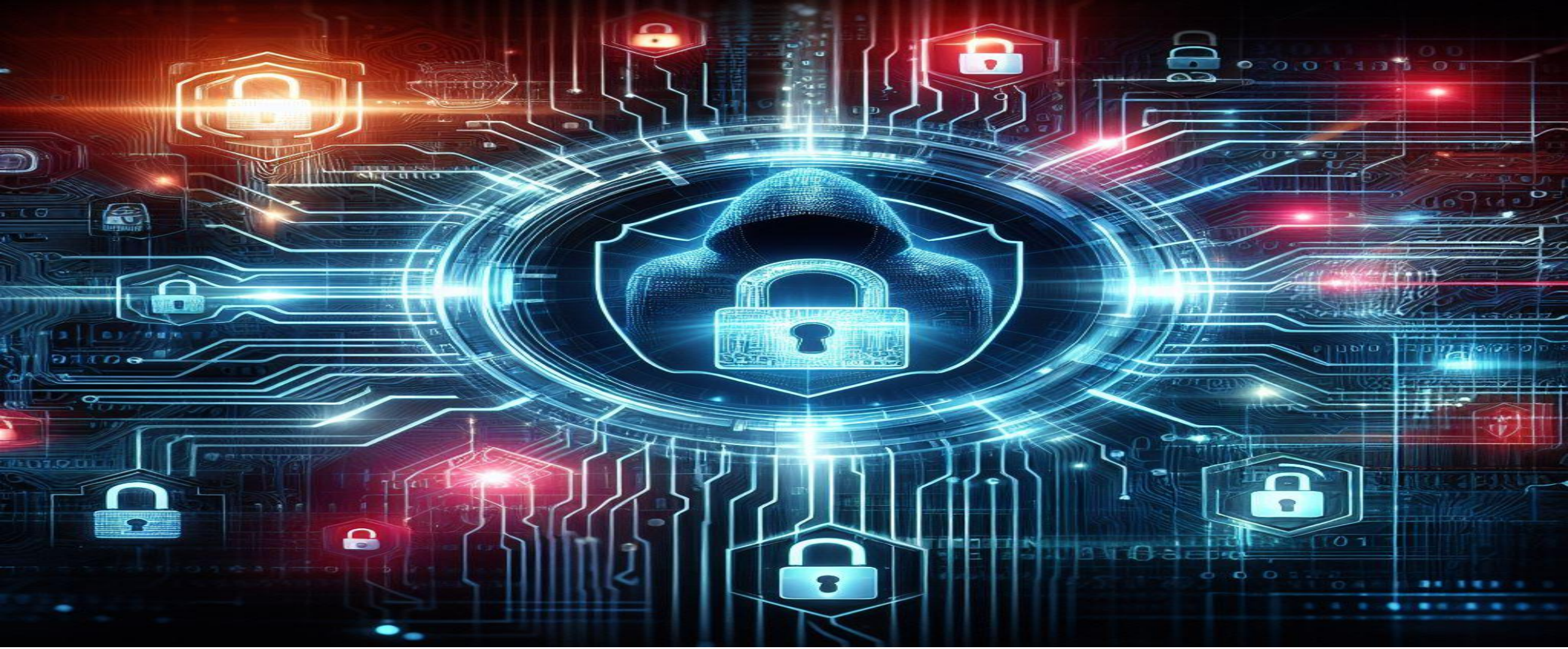


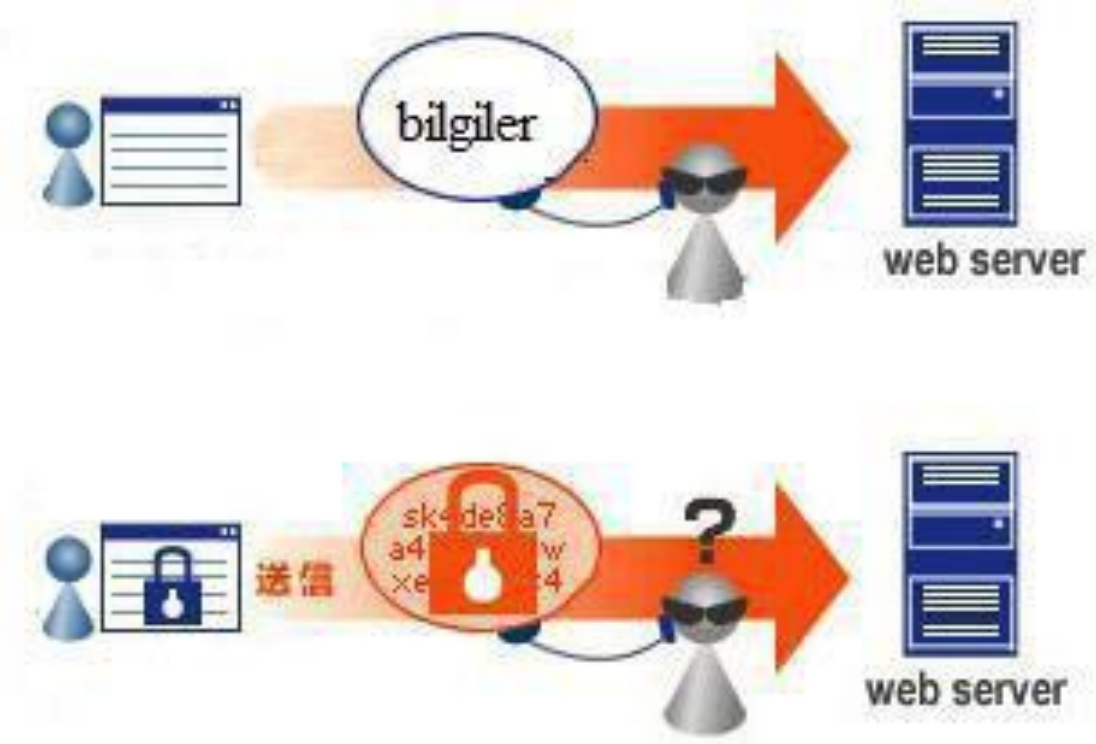
NETWORK SECURITY

Lecturer Erhan AKAGÜNDÜZ

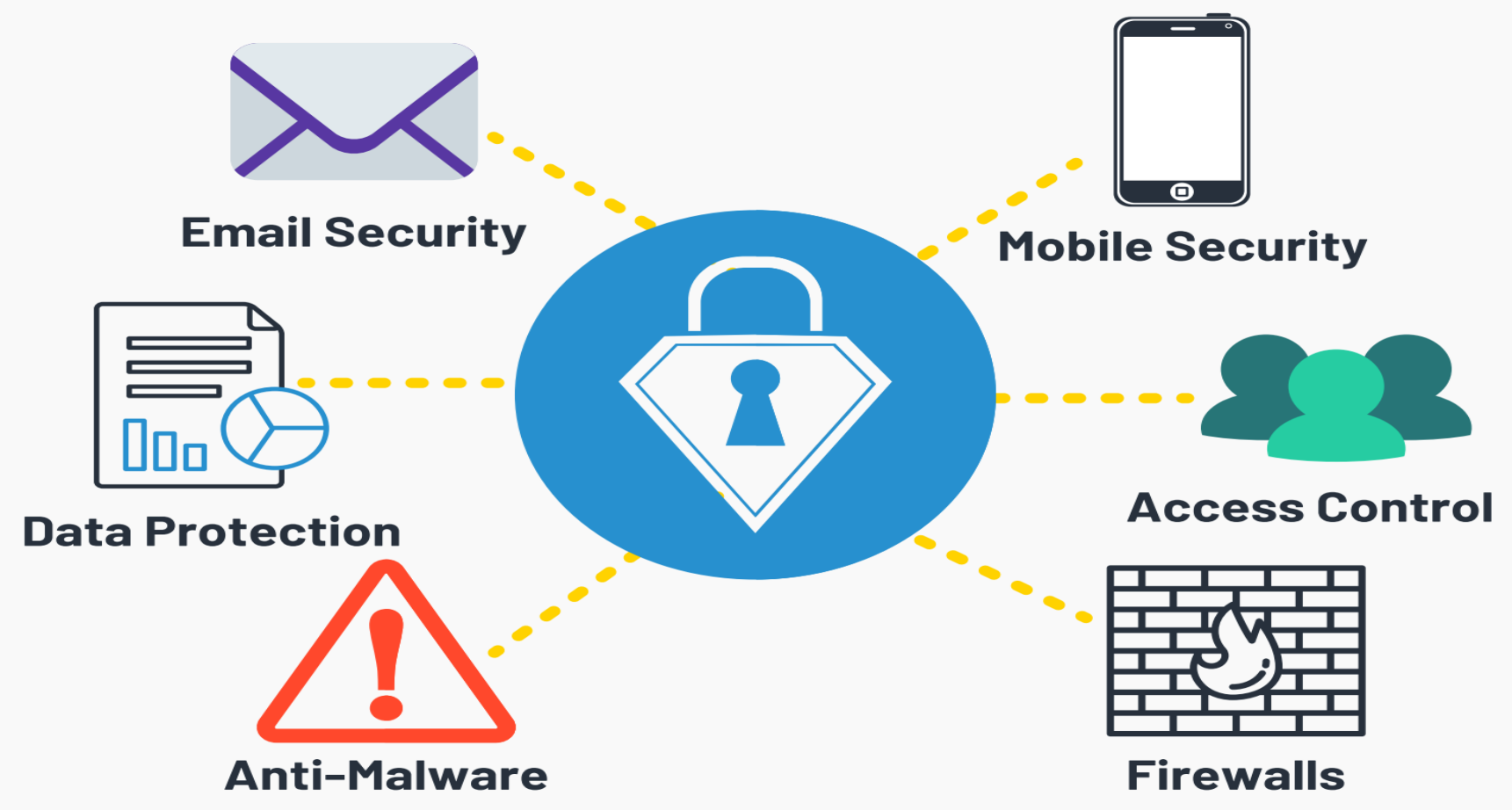
NETWORK SECURITY

- ✓ Bilgisayar ağlarının yaygınlaşması, İnternet aracılığı ile elektronik işletmelerin ortaya çıkması ve internet üzerinden ticaretin yaygınlaşmasıyla birlikte bilgisayar ağları oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır.
- ✓ Ağlardaki bu zayıflıklar iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmaktadır.

NETWORK SECURITY



NETWORK SECURITY



NETWORK SECURITY

- ✓ İnternet ağı kişisel veya iş ilişkileri arasında bilgi akışını sağlayan ve düzenleyen bir iletişim aracı hâline gelmiştir.
- ✓ İnternet üzerinde bilgi kaybı olabilir veya gizlilik ihlal edilebilir. İnternet üzerindeki bu tür güvenlik açıklıkları kullanıcıları İnternete karşı güvensizleştirebilir.

NETWORK SECURITY

- ✓ Bu sorun da web tabanlı şirketler için büyük risk olur.
- ✓ Bu tür güvenlik açıklıklarına karşı önlem almak kişisel kullanıcılar ve şirketler için gündeme gelmiştir.

NETWORK ATTACK RISKS

- ✓ Kablolu veya kablosuz tüm bilgisayar ağları günlük kullanımda önemli bir yer tutmaktadır.
- ✓ Bilgisayar sektöründe çalışanlar, zamanın çoğunu bilgisayar başında geçirmektedir.
- ✓ Aynı zamanda bireyler ve kuruluşlar da bu sektörde çalışanlar gibi e-posta, düzenleme, dosya yönetimi, hesaplama gibi farklı işlevler için bilgisayarları ve ağlarını kullanmaktadır.

NETWORK ATTACK RISKS

- ✓ Güvensiz bir ağda yetkisiz bir kişinin saldırısı yüksek maliyetli ağ kesintilerine yol açabilir.
- ✓ Saldırıyı gerçekleştirenler, yazılımın zayıflıkları, kullanıcı adına ve bu kullanıcıya ait parolayı tahmin etme ve donanım saldırıları gibi daha düşük düzeyli teknik yöntemlerle kolayca ağa erişim kazanabilir.

INFORMATION THEFT

- ✓ Bilgi hırsızlığı izinsiz ağa erişimin, korumalı ağ bilgilerini elde etmek amacıyla kullanıldığı bir saldırıdır.
- ✓ Saldırgan, bir sunucuda veya bilgisayarda, daha önce kimlik doğrulaması için çaldığı bilgileri kullanabilir ve dosyalarda saklanan verileri okuyabilir.

INFORMATION THEFT

- ✓ Saldırgan, ağ iletişimlerini izleyen ve veriyi yakalayan bir aygıt veya program olan, donanım veya yazılım tabanlı paket yoklayıcı kullanarak ağ ortamında geçiş hâlindeki veriyi çalabilir.
- ✓ Bu tür yapılan bilgi hırsızlığı yasak olarak ülkemizde suç kabul edilmektedir.
- ✓ Tescilli bilgilerin çalınması, bilgisayar kullanarak ekonomik dolandırıcılık, bilgi veya ağların sabotajı Türkiye Cumhuriyeti kanunlarında suç kabul edilmektedir.

INFORMATION THEFT

IDENTITY THEFT

- ✓ Kimlik hırsızlığı, kişinin izni olmadan kişisel bilgilerinin elde edilmesidir.
- ✓ Kimlik hırsızlığını kullanılarak kişinin kredi kart numarası, ehliyet numarası, vatandaşlık numarası, internet bankacılığı bilgileri, e-posta şifre parolası ve önemli diğer kişisel bilgilerin bir başkası tarafından çıkar sağlamak amacı ile yapılan dolandırıcılık türüdür.
- ✓ TCK'ye göre bu suç sayılmaktadır.

IDENTITY THEFT

- ✓ Kimlik hırsızlığına uğranılmış ise bu birkaç yoldan anlaşılabilir:
  - ❑ İzinsiz çevrim içi satın almalar yapıldığında,
  - ❑ Kişi üzerinden çeşitli kurumlarda kredi veya telefon hattı başvuruları sonucu borçlanma bilgileri geldiğinde,
  - ❑ Kişinin bilgi dahilinde olmadan sosyal paylaşımlar olduğunda.
- ✓ Bu gibi durumlarda adli mercilere başvurmak gerekmektedir.

DATA LOSS AND DATA USE

- ✓ Kişisel bilgisayarlar ve işletmelerde kullanılan bilgisayarlarda veriler elektronik ortamda saklanmaktadır.
- ✓ Bu verilerin erişilemez veya kullanılamaz hâle gelmesine veri kaybı adı verilmektedir.
- ✓ Veriler ağdaki bilgisayarlar üzerinde saklanabilir veya yedeklenebilir.

DATA LOSS AND DATA USE

- ✓ Herhangi bir bilgisayar ağına gönderilen veri, o veriyi almaya yetkisi olmayan kişilerce ele geçirilebilir.
- ✓ Bu kişiler iletişimi gizlice gözetleyebilir ya da gönderilen bilgi paketini değiştirebilir.
- ✓ Bunu birçok metod kullanarak yapabilir.
- ✓ Örneğin, bilgi iletişiminde bir alıcının IP numarasını kullanarak sanki o alıcıymış gibi gönderilen verileri istediği gibi kullanabilir.

SERVICE DISRUPTION

- ✓ Kişisel veya işletmelerdeki kullanıcıların yasal haklarını kullanmalarını engelleme olarak tanımlanabilir.
- ✓ Ağ haberleşmesinde kullanıcı adı ve parolasını kullanamaması, kullanıcıların web hizmetine bağlanamaması gibi durumlarda ağa dışarıdan müdahale olduğu anlaşılabilir.

NETWORK COMMUNICATIONS THREATS

- ✓ Bilişim teknolojilerindeki gelişmeler kullanıcılara büyük kolaylık sağlarken aynı zamanda pek çok tehdidi de beraberinde getirmektedir.
- ✓ İletişim ağlarında ki güvenlik açıkları kullanıcıların sisteminin ele geçirmekten öte kişisel bilgileri ve büyük firmaların gizli bilgilerini ele geçirilmesine ve bu sayede maddi kazançlar elde etmeye yönelik olmaya başlamıştır.

NETWORK COMMUNICATIONS THREATS

- ✓ Yeni nesil tehditler kullanıcılardan, güvensiz ağlardan kaynaklanabilir.
- ✓ İnternetin genişlemesi ile beraber ağ uygulaması da beklenmedik şekilde genişlemiştir.
- ✓ Bu gelişmeyle birlikte ağ kurulup işletmeye alındıktan sonra ağ yönetimi ve ağ güvenliği büyük önem kazanmıştır.

NETWORK COMMUNICATIONS THREATS

- ✓ Çünkü internete bağlı ağ sistemleri arasında dolaşan hiçbir veri gerekli önlemler alınmadığı takdirde güvenli değildir.
- ✓ Ağın güvenilir biçimde çalıştırılması anahtar sözcük konumuna gelmiştir.
- ✓ Çünkü ağın günümüz teknolojisi ile kurulup çalıştırılmasıyla iş bitmemekte esas iş ağ performansının ve güvenilirliğinin sağlanmasında bitmektedir.

NETWORK COMMUNICATIONS THREATS

- ✓ Genellikle ağ yapısına yapılan saldırıların çoğu iç ağdan gelir.
- ✓ Ağa açılan bilgisayarın verdiği hizmete göre ne tür saldırıya uğrayacağı ve saldırı türleri de ortaya çıkabilir.
- ✓ Ağa yapılan saldırılar donanıma veya yazılıma yönelik olabilir.

NETWORK COMMUNICATIONS THREATS

- ✓ Donanıma yönelik saldırılarda veri depolama kaynaklarına veya ağ cihazlarına yönelik olabilir.
- ✓ Yazılıma yönelik saldırılar ise kullanıcı verilerine erişim sağlamak için olabilir.
- ✓ Potansiyel saldırı kaynakları, bilgisayarın bağlı olduğu geniş ağ üzerinden, İnternet bağlantısı üzerinden, modem havuzu üzerinden olabilmektedir.

EXTERNAL AND INTERNAL THREATS

- ✓ Harici tehditler, ağ dışında çalışan kullanıcılardan gelir. Bu kişilerin bilgisayar sistemlerine veya ağa yetkili erişimi bulunmamaktadır.
- ✓ Harici saldırganlar, ağa saldırılarını genellikle İnternet üzerinden, kablosuz ağlardan veya çevirmeli erişim sunucularından gerçekleştirir.
- ✓ Bu saldırılar maddi ve manevi zarara yol açar ve engellemek için güvenliğin arttırılması gerekir.

EXTERNAL AND INTERNAL THREATS

- ✓ İstemci-sunucu ortamında ağ yöneticileri çok farklı bir savaşın içindedir.
- ✓ Ağlarındaki her erişim noktasından saldırılara açıklar.
- ✓ İnternet çok sayıda sistemin birbirine bağlanmasını sağlayarak kendine özgü problemleri de beraberinde getirmiştir.

EXTERNAL AND INTERNAL THREATS

- ✓ Dâhili tehditler ise; bir kullanıcının hesabı üzerinden ağa yetkisiz erişimi olduğunda ya da ağ ekipmanına fiziksel erişimi olduğunda gerçekleşir.
- ✓ Dâhili saldırgan, ilkeleri ve kişileri tanır.
- ✓ Bu kişiler genellikle hangi bilgilerin ve savunmasız olduğunu ve bu bilgileri nasıl elde edebileceğini bilir.

EXTERNAL AND INTERNAL THREATS

- ✓ Fakat, dahili saldırılar her zaman kasıtlı olmaz.
- ✓ Bazı durumlarda, dahili bir tehdit, ağ dışındayken bilmeden dahili ağa virüs veya güvenlik tehdidi getiren güvenilir bir çalışandan da gelebilir.
- ✓ Güvenlik, dâhili ağlarda da önemli bir konudur.
- ✓ Firma çalışanları bazen veri hırsızlığı yapabilir ya da sisteme virüs bulaştırabilir.

EXTERNAL AND INTERNAL THREATS

- ✓ Bir işletmedeki bazı çalışanlar, ağa bağlanmak için kullandıkları şifre, kötü niyetli çalışanlar (cracker) tarafından tahmin edilebilir şekilde seçerlerse bu bir güvenlik açığı oluşturur.
- ✓ Veya yalnızca merkezde bir güvenlik duvarı ile korunan ve bu merkeze özel kiralık devre ile bağlı bulunan bir şubede, herhangi bir kullanıcının telefon hattı ile İnternete bağlanması da bir güvenlik açığı oluşturabilir.

EXTERNAL AND INTERNAL THREATS

- ✓ Bazı firma çalışanları da yanlışlıkla İnternetten ya da floppy diskten bir belge yüklerken bilgisayara virüs bulaştırabilir ve kendi bilgisayarına bulaştırdığı virüsün farkına varmadan ağ içindeki diğer bilgisayarlarla bilgi alışverişi ile bu virüsü tüm ağa yayabilir.
- ✓ Bu soruna karşı alınabilecek önlem, tüm bilgisayarlara virüs koruma programı yüklemek ve bir belge yüklerken ekrana uyarı mesajları gelmesini sağlamaktır.

EXTERNAL AND INTERNAL THREATS

- ✓ İşletmede çalışan meraklı kullanıcılar casus gibidir.
- ✓ Bu kullanıcı diğer çalışanlarla arasındaki rekabet nedeniyle, erişim yetkisine sahip olmadığı bir takım gizli bilgilere ulaşmaya çalışır.
- ✓ Mesajlara ya da maaş bilgilerine erişmek masum olabilir ancak önemli ve gizli finansal bilgilere ulaşmak, o şirket için büyük tehlike oluşturabilir.

EXTERNAL AND INTERNAL THREATS

REFERENCES

Ağ Temelleri Ders Modülleri– MEGEP MEB (2011)