"Siber güvenlik devlet politikası olmalı, yerli yazılım öne çıkmalı"

Günümüzde elde edilen her türlü bilgi, teknoloji altyapıları, bilgisayar ağları ve internet vasıtasıyla kitlelere hızla yayılıyor. Sanal dünyada en değerli varlığımız haline gelen bilgi akışının daha güvenli bir şekilde yayılmasını sağlamak, bilgiye yönelik tehditleri önlemek için tüm kurumlar bir dizi tedbir almak durumunda. Bilişim sistemleri kullanımının 2000'lerde yaygınlaştığı Türkiye, dünya standartlarında bir bilgi güvenliğine ulaşmak istiyorsa, bu konuda ulusal düzeyde bir politika geliştirmek zorunda. Bilgi Güvenlik Akademisi (BGA) Yönetim Kurulu Başkanı Huzeyfe Önal, "Türkiye'de bilgi güvenliğinin önündeki en büyük engel sadece ürün odaklı ve dışa bağımlı bir anlayışın hakim olması. Bilgi güvenliği işi yapan firmaların yüzde 90'ı sadece al sat işi, yani bilgi güvenliği ticareti yapıyorlar. Yerli yazılım üretimi yapan ve bilgi güvenliğinin ticari değil, stratejik önemini anlayan firmaların artması bu alanda olumlu bir yaklaşımı beraberinde getirecek" diye konuştu.

Huzeyfe Önal / Bilgi Güvenlik Akademisi (BGA) Yönetim Kurulu Başkanı

Türkiye'de bilgi güvenliği konusunun gelişmesinin önündeki en büyük engel, ürün odaklı ve dışa bağımlı bir anlayışın yaygın olması. Bu engeli aşmanın yolu ise yerli üretim yapan şirketlerin ve bilgi güvenliğinin ticari öneminin yanı sıra stratejik önemini de keşfeden firmaların sayısını artırmaktan geçiyor. Bu sayımızda Bilgi Güvenlik Akademisi (BGA) Yönetim Kurulu Başkanı Huzeyfe Önal ile "Bilgi Güvenliği ve Teknolojileri" konusunu irdeledik.

Bilgi güvenliği derken neyi kastediyoruz? Günümüzde bilgi güvenliği neleri kapsıyor?

Bilgi güvenliği, günümüzde çok geniş bir alanı kapsayacak şekilde tanımlanmış olan "bilgi" kavramının güvenliğiyle ilgili her konuyu kapsar. Değer ifade eden her tür veri bilgidir ve korunmalıdır. Bilgi güvenliği denildiğinde genellikle akla bilişim güvenliği gelir ve bu iki kavram sık sık birbirinin yerine kullanılır. Oysa bilgi güvenliği kavramı, bilişim güvenliğini de içeren çok daha geniş bir kavramdır. Bilişim sistemlerinin kullanılmadığı, hatta teknolojinin hiç kullanılmadığı ortam ve zamanlarda da bilgi kavramı mevcuttu ve bunun güvenliğinin sağlanması için çalışmalar yapılıyordu.
Bilginin gizliliğini sağlamak için sıkça kullandığımız şifreleme algoritmalarının geçmişine bakacak olursa teknolojinin keşfedilmesinden çok önceye dayandığı görülür. Ama günümüzde bilgi demek biraz da bilişim demek olduğu için, farklı olduğunu bilsek de, çoğu zaman bilişim güvenliği yerine bilgi güvenliği kavramını kullanmayı tercih ediyoruz.
Son zamanlarda özellikle medyaya yansıyan şekliyle siber güvenlik kavramı da gündemimizde oldukça fazla yer bulmaya başladı. Bilgi güvenliği ve siber güvenlik tanımları çoğu noktada birbiriyle çakışsa da, bilgi güvenliği siber güvenlikten oldukça farklı ve geniş bir kavramdır. Siber güvenlik adı üzerinde, sadece siber dünyayı ve bunun etkileyeceği alanları kapsıyor.

Bilgi güvenliğinde hedef nedir? Göz önünde tutulması gereken temel ilkeler nelerdir?

Bilgi güvenliğinde amaç, bilgi olarak tanımladığımız değerli verilerimizin gizlilik, bütünlük ve ulaşılabilirliğinin sağlanmasıdır (C.I.A prensibi). Bir bilginin güvenli olduğunu söyleyebilmek için bu üç şartı sağlaması gerekir.
Burada bilişim dünyasında sık kullanılan yanlış bir algıyı da belirtmek lazım: "En güvenli sistem fişi çekilmiş sistemdir." Evet, fişi çekilmiş sistem kendisi için güvenlidir fakat genel çerçeve açısından değerlendirildiğinde fişi çekilmiş sistem kimseye hizmet veremeyeceği için bilgi güvenliğinin en temel prensibi olan erişilebilirlik, ulaşılırlık özelliğini sağlamayacaktır.
Bilgi güvenliğinde amaç bilgiyi her türlü olumsuzluğu göze alarak bilginin güvenliğini sağlamak değil, bilgiyi kullanılabilir halde güvenli tutmaktır. Bilgi güvenliği ve kullanım kolaylığı ters orantılıdır, güvenliğe çok önem verirseniz kullanışlılık seviyesi düşer, güvenliğe çok önem vermezseniz kullanım kolaylığı artar. Burada dengeyi gözetmek gerekir.

Bilgi güvenliği ve teknoloji sistemlerinin kurulma aşamalarından bahseder misiniz?

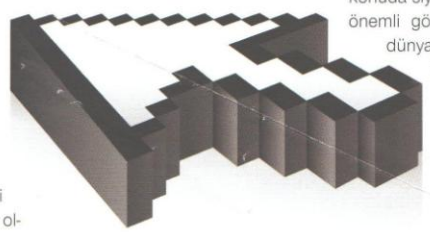
Günümüzde bilginin güvenliği teknolojinin yaşam döngüsünde en sonda yer alır. Yani önce ihtiyaç belirlenmekte, araştırılmakta, teknoloji kullanılmakta ve en sonda bunun eksi yanları, güvenlik açısından sakıncaları ortaya çıkarılmakta ve günü kurtaracak çözümlerle bu sorunlardan kurtulmaya çalışılmaktadır. Bu durum teknolojinin işleyişini tam kavrayamamış kişi ve kurumlarda sık rastlanan hatalı bir yaklaşımdır. Bilgi güvenliği daha teknolojiyi üretirken ve kullanmaya başlamadan dikkate alınması gereken önemli bir olgudur. Eğer proaktif bir yaklaşım sergileyerek başında önlem alırsanız güvenlikle ilgili yaşanacak sıkıntılar da o oranda azalacaktır.
Günümüzde kurumlara bilgi güvenliği ile ilgili standartlar önerilmektedir. Bu standartların başında ISO 27001 bilgi güvenliği yönetim standardı gelmektedir. Bu standartla birlikte kurumlar bilgi güvenliğinde temel seviyede bir bilgi birikimine ve işleyişe sahip olduklarını kanıtlamış olur. Fakat burada düşülen başka bir hata sertifikasyonların sadece kâğıt üzerinde kalma riski-

dir. Standarda sadece dostlar alışverişte görsün mantığıyla yaklaşılırsa bilgi güvenliği açısından duvarda asılı bir kâğıt parçasından farkı kalmayacaktır.

Bilgi güvenliğinde Türkiye hangi noktada? Yetersizse sizce ne yapılması gerekiyor?

Türkiye 2000'li yıllarla birlikte bilişim sistemlerinin yaygınlaştığı bir ülke olduğu için henüz dünya standartlarında bir bilgi güvenliği anlayışına sahip değil. Bununla birlikte Türkiye'nin teknoloji ve buna bağlı konulara adaptasyon süreci normalin üzerinde olduğu için bilgi güvenliği konusunda da hızla yol almıştır.

Türkiye'de bilgi güvenliği konusunun gelişmesine engel en önemli konulardan biri sadece ürün odaklı ve dışa bağımlı bir anlayışın yaygın olmasıdır. Türkiye'de bilgi güvenliği işi yapan 40'a yakın firma bulunuyor. Bu firmaların yüzde 90'ı sadece al sat işi, yani bilgi güvenliğinin ticaretini yapıyor. Yerli üretim yapan firmaların sayısı ve bilgi güvenliğinin sadece ticari değil, stratejik önemini anlayan firmaların sayısı arttıkça Türkiye'deki bilgi güvenliği yaklaşımı da olumlu yönde gelişecektir. Kamu tarafına bakacak olursa orada da ciddi bir bilinçlenme söz konusu fakat söylemden eyleme geçiş bir türlü gerçekleşemiyor. Bunun da temel sebebi ulusal seviyede bir bilgi güvenliği politikasının olmaması ve kurumların bilgi güvenliği konusunu klasik bir IT işi gibi görmeleridir.



Türkiye'de bilgi güvenliği konusunda kamuoyundaki farkındalığı yeterli buluyor musunuz?

Türkiye, gündemin normalin üzerinde bir hızla değiştiği bir ülke. Dolayısıyla bilgi güvenliği, siber güvenlikle ilgili konular medyada hak ettiği önemi göremiyor. Mesela Wikileaks sızıntısına benzer çok daha küçük çaplı ama etkileri açısından oldukça ciddi siber güvenlik olayları yaşanıyor. Ancak, bu olayları genellikle ulusal medyada göremiyoruz. Bunun temel nedeni günümüzdeki medya yöneticilerinin bilişim dünyasının ve siber güvenliğin önemini tam kavrayamamış olması ve işin magazinsel kısmını ön plana çıkarıyor olmasıdır. Oysa Türkiye ile eş değer diğer ülkelere bakıldığında bu tip olayların çok ciddi bir şekilde incelendiğine ve ders çıkarılarak acil önlemler alındığını görebiliriz.

Farkındalığının artırılmasında medyanın dışında kimlere görev düştüğü kanaatindesiniz?

Sadece medyaya görev düşmüyor tabii ki. Bu konuda siyasi partilere de oldukça önemli görevler düşüyor. Bugün dünyanın süper güç olarak tanımladığı ABD'de, bilgi güvenliği konusuna en üst düzeyde önem verildiğini göstermek için devlet başkanının ulusa sesleniş konuşmalarından biri siber

e ayrılmıştır. Medya ve siyasilerin hari- il toplum kuruluşlarının ve bilgi güvenliği ş yapan firmaların da farkındalığı artırma da çalışmalar yapması önemlidir. BGA r yıl 20'nin üzerinde bilgi güvenliği etkin- tkıda bulunuyoruz.

de bilgi güvenliği konusunu daha ileri e taşımak için önerileriniz var mı?

ülkelerin büyük çoğunluğu siber güven- ijisini yayımlamıştır ve buna uygun hare- ektedir. Bugün, konunun en sıcak olduğu ın yaşıyoruz. Birkaç yıl sonra bu konuya ermeye başladığımızda treni birkaç istas- çırmış olacağımızı düşünüyorum. Siber k alanında sözü geçen uluslararası bir güç una erişmek hedefimiz olmalı ve bu hedef et politikası olarak benimsenmelidir.

nüfusu genç ve dinamik bir ülke. Bu ufusun hacking olaylarına karşı merakı da sek. Bu konuda gerçekleştirilecek formal rle bu gençlerin sektöre kazandırılması 'nin siber güvenlik konusundaki dışa ba- nı önemli oranda azaltacaktır. Yerli siber k yazılımı/donanımı üreticilerine özel teş- verilmesi ve bu konuda araştırma yapan- aylık tanınması da bu konuda yatırım yapa- çalışacaklara ek motivasyon sağlayacağı mlidir.

uda atılması gereken önemli bir adım da özel sektör ve üniversitelerin siber güvenlik unda iş birliği yapmasıdır. Özel sektör talebi ihtiyacı belirleyen, kamu, buna uygun yö- leri hazırlayan, üniversiteler de bu ihtiyaç- recek insan kaynağına sahip olan önemli erdir.

yıl sonra, örneğin 2015'te bilgi gü- dünyası neleri konuşuyor olacak?

konuştuklarımızdan çok da farklı konuları mayacağımızı düşünüyorum. Zira dünyanın internetı aynı zaman diliminde aynı şart- llanmıyor ve bazı şeylerin doğası hiç de- er.

hâlâ altı yedi sene öncesinin wormları in- dolanıyorsa, bugünkü bazı wormlar da sene sonra yine dolanıyor olacak. On nce kullanıcılar kandırılarak sistemlerine m yükleniyordu, aynı yöntem hâlâ en ge- rcih edilen yöntemlerden biri. Saldırıların kli değişse de, özünde hep aynı amaca ediyor. Yine temel bilgi eksikliğinden do- enlik konusu yakında çıkmaza girecek. her konuda yeni ürün, yeni katman alan güvenlik uzmanları yakın zamanda artık güvenlik sistemlerinin yönetilemez olduğunu anlamaya başlayıp daha basit sistemlere yönelecek. Basitlik *güvenliğin* sağlanmasında önemli bir bileşendir.

Bunların haricinde bilgi güvenliği kavramının oluşmasının temel nedeni olan siber saldırganların çalışma şekilleri incelendiğinde, nerede daha çok kullanım varsa o alanlara yönelik yeni saldırıların geliştirildiğini görebiliyoruz. Bu da ilerleyen zamanlarda saldırıların bilgisayar kullanıcılarından mobil sistem kullanıcılarına yöneleceğini işaret ediyor.

Mobil sistemler bilgisayarlardan farklı olarak her zaman yanımızda taşıdığımız sistemler olduğu için bilgisayarlardan çok daha tehlikelidir. Bugün bir akıllı telefona yüklenecek zararlı bir yazılımla bir kişinin 7/24 takibi yapılabilir, uzaktan telefonun mikrofonu ve kamerası açılarak kayıt yapılabilir. Bunlar da saldırganların iştahını kabartıyor.

Önümüzdeki yıllarda sıkça karşılaşacağımız önemli bir konu da DDoS (servis erişimi durdurma) saldırılarıdır. Bu saldırı tipi ileri seviye uzman bilgisi gerektirmez ve hedef sistemlerin internet üzerinden ulaşılamaz olmasını sağlamak için gerçekleştirilir. Saldırganların ve saldırı yöntemlerinin hızla gelişmesi ve değişkenlik göstermesi, bu konuda saldırgan mantığıyla olaya yaklaşıp proaktif güvenlik önlemleri almayı kolaylaştıracak yeni bir meslek dalı olan "beyaz şapkalı hacker"lığın önümüzdeki yıllarda sektörde en fazla ihtiyaç duyacağı kariyer alanlarından biri olacağını belirtmek gerekir.