Oğuz YILMAZ
Labris Networks CTO

"IoT, m2m, 4G gibi kavramların hayat bulmasıyla artık siber dünyanın sınırları en uç noktalara taşınıyor. "İnternet hayattır" söylemi gerçekten hem ekonomik hem de güncel hayatımız ele alındığında karşılığını bulmuş oluyor."

"Along with nascence of concepts such as IoT, m2m and 4G, limits of cyber world moves to extremum points. 'Internet is life' expression really corresponds when both economic and daily lives of us are handled."

Labris NETWORKS

Kurumların en büyük hazinesinin, verilerinin ve işlerinin sürdürülebilirliği olduğunu vurgulayan **Labris Networks CTO Oğuz YILMAZ**, "Eğer bir siber korsan en önemli verilerinizi ele geçirirse, o an verilerinizi geri almak için nasıl bir meblağı gözden çıkarabileceğinizi düşünün. İşte bilişim güvenliği çözümleri, bu meblağın çok çok küçük bir parçasına mal oluyor ve sizi belki de şirketinizin faaliyetlerini durdurmanıza yol açacak bir süreçten sakınıyor. Olası bir sızıntı ya da veri kaybının yaratacağı felaketin boyutları göz önüne alındığında bilişim güvenliğinin önemi açık seçik gün yüzüne çıkıyor. Tüm dünyada bilişim suçlarının ekonomiye etkisi 400 milyar doların üzerinde. Siber suç çeteleri 2015 Siber Güvenlik Öngörüleri raporumuzda da belirttiğimiz gibi artık şirketleri hedef alır hale geldiler. Yan bir şirketi hedef alarak, öncelikle ele geçirme yöntemleri ile şirketi

*Emphasizing that the most valuable treasure of corporations is sustainability of data and business, **Labris Networks CTO Oğuz YILMAZ** says "Imagine how much 'money' you can spend to take your data back if a cyber pirate captures the most important data of you. But information security solutions cost very small part of this 'money' and maybe protect you from a process that can make you stop activities of your company. Considering the extent of the disaster that can be caused by a potential sneak or data loss, importance of information security comes to light. The effect of cybercrimes on economy around the world is over 400 billion dollars. As we have mentioned in 2015 Cyber Security Forecasts report, cybercrime bands started to target companies anymore. By targeting a branch company, firstly they try to leave*

(/padphoto/49251890/20/afd23c93-a1c0-e311-b0d5-001a6465f174)

Sayfa: 21

zor durumda bırakmaya çalışıyorlar. Örneklere baktığımızda özellikle yönetici ve yüksek yetki seviyeli kişilerin bilgisayarlarının hedef alındığını görüyoruz. Dolayısıyla ister kişilerin kendi cihazları olsun, ister kurumun sağladığı cihazlar olsun, bunların hem kurum içinde hem de kurum dışında güvenliği aslında kurum siber güvenliğinin bir parçası haline geldi." dedi.

Yılmaz, sözlerine şöyle devam etti: "Tehditlerin çok hızlı geliştiği siber tehdit ortamında, bu tehditleri alt etmek için sizin de kendinizi sürekli geliştirmeniz ve bilgilerinizi güncel tutmanız gerekiyor. Oluşabilecek saldırılara karşı her daim hazır olmak amacıyla kurduğumuz "Labris Security Operations Center"da siber tehditleri ve yayılımları takip ediyor, CWL Lab'da (Cyber Warfare Lab) siber savunma araçlarının en önemli analiz ve karar bileşenlerini geliştiriyoruz. Tehdit geliştikçe biz, biz geliştikçe bizim çözümlerimizi kullananlar da gelişiyor ve siber tehditlere karşı daha güvenilir oluyor. Yaygın bir sensör ağı da tehditlerin en erken fark edilmesini sağlıyor. Buna ek olarak siber olaylara müdahale merkezlerinin (SOME) oluşturulması, yaygınlaştırılması, ticarileştirilmesi de bunun ayrı bir boyutu. Ülke olarak SOME konusunda da başlangıç aşamasındayız. Biz üretici olarak HARPP DDOS CERT ile ekspertizimizi DDOS saldırılarına karşı müşterilerimiz ile paylaşmaya bundan 3 yıl önce başladık ve şu anda ekosistemimizi genişletip bilgilerimizi paylaşarak daha fazla firmanın da buna erişmesini sağlamak için çalışıyoruz. Resmi değerlendirdiğinizde zayıf noktamız şu anda bilinçli hareket edilmemesi sonucu oluşan büyük bir süreç, araç ve ekip açığı. Gerektiğinde ihtiyacınız olan müdahale yardımını verebilecek ekiplerin sayısının az olması ya da olmaması ise diğer bir büyük zafiyet. İşte profesyonel güvenlik yönetim ekipleri olarak bunları tamamlıyoruz."

Tehdit algısının artması ve sektörün sağladığı katma değerin devlet başkanları seviyesinde farkındalığa sahip olmasının bilişim güvenliği sektörünü çok daha hızlı büyüteceğini, inovasyon temelli yaklaşımlarla ürün altyapılarının sürekli bir değişim ve gelişim içinde olacağını ifade eden Yılmaz, şunları ekledi: "Geçtiğimiz 10 yılda bilişim teknolojilerinden uzak olmanın ekonomiye maliyetini konuşuyorduk. Çok kısa bir süre içinde güvenli olmayan bilgi işlem altyapılarının ve güvenliği sağlanmadan sayısallaştırılan ve biriktirilen bilginin ekonomiye

the company in a tight spot. Looking at the examples, we see that especially computers of managers and people with high echelons are targeted. Consequently, internal and external security of personal devices or devices offered by a company has been a part of corporate cyber security."

Yılmaz continues his words: "In cyber security environment that threats are raising at fast pace, you should always improve yourself and keep up-to-date your information to overcome these threats. In 'Labris Security Operations Center' which we established with the aim of being ready against any attacks, we follow cyber threats and propagations and in CWL Lab (Cyber Warfare Lab) we develop the most important analysis and decision elements of cyber defense tools. As threats rise we develop, as we develop people who use our solutions progress and become safer against cyber threats. A prevalent sensor network lets early detection of threats. In addition to these, establishment, popularisation and commercialisation of cyber events response centres is another dimension. As the country, we are at start-up phase in terms of cyber events response centres. As a producer, three years ago we started to share our expertise against DDoS attacks via HARPP DDOS CERT and now we are trying to provide more companies' access by extending our ecosystem and sharing our information. Evaluating this picture, our weak point is a big process arising of unconscious acts, tool and team deficit. Having none or less team to response when needed is another weakness. Here, we as professional security management teams overcome these deficiencies."

Stating that increasing threat perception and awareness on value added created by this industry even at president level will grow information security industry even faster and product infrastructures will be in a continuous change and progress based on innovation oriented approaches, Yılmaz adds: "In the last 10 years, we were talking about financial expense of being far apart from information technologies.

(/padphoto/49251891/21/afd23c93-a1c0-e311-b0d5-001a6465f174)

Sayfa: 22

maliyetini konuşmaya başladık. IoT, m2m, 4G gibi kavramların hayat bulmasıyla artık siber dünyanın sınırları en uç noktalara taşınıyor. "İnternet hayattır" söylemi gerçekten hem ekonomik hem de güncel hayatımız ele alındığında karşılığını bulmuş oluyor. Bu hayatın güvenli olması, bilişim güvenliğinden geçecek. Verilerin güvenliği noktasında elbette kurumlar zamanla daha farkında olacaktır ancak ülke olarak kanunlarla da bunun desteklenmesi gerekir. Bu anlamda kişisel verilerin korunması ile ilgili kanun çalışmalarının uluslararası standartlar seviyesinde tamamlanmasını elzem görüyoruz."

In a short span of time, we started to talk about financial cost of unsafe data processing infrastructures and digitized and saved information without security. Along with nascence of concepts such as IoT, m2m and 4G, limits of cyber world moves to extremum points. 'Internet is life' expression really corresponds when both economic and daily lives of us are handled. Security of life is subject to information security. In terms of data security, corporations will be more aware but we should support this via law. In this sense, it is vital to complete law studies about personal data protection at international standards level."

Yılmaz, sözlerini şöyle noktaladı: "BYOD aslında bir yandan da bulut bilişimin gelişmesi ile destekleniyor. Mobil cihazlardaki kurumsal uygulamalar da her yerden ulaşılır bulut servisleri üzerinden çalışıyor. Dolayısıyla bu bulut servislerinin kesilmeden ve yavaşlamadan devam etmesi de oldukça önemli. Siber saldırılar içinde en önemli tehdit, hizmetleri tamamen kesmeye ya da yavaşlatmaya yönelik olan DoS (Denial of Service) ve DDoS (Distributed Denial of Service) saldırıları. Bu saldırıların ilk başta Telekom operatörleri seviyesinde çözülebileceği şeklinde oluşan yanılgı son dönemde yok oldu neyse ki. Kurumun kendi veri merkezinde detaylı DDOS paket inceleme yapabilen ekipmanlara bir hibrid anti-ddos topolojisinin gerektiğini dünya gelişmeleri gösteriyor. Bu noktada da kurumlar maalesef geciken yatırımlarını tamamlayarak hibrid (Telekom + Kendi veri merkezi) DDOS güvenlik topolojisini oluşturmalıdır."

Yılmaz concludes saying, "In the meantime, BYOD is supported by development of cloud computing. Enterprise applications on mobile devices operate on cloud services accessible everywhere. Consequently it is also very important that cloud services should continue without interruption or slowdown. The most important threats between cyberattacks are DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks which aim to cut or slow down services. Fortunately the mistake of thinking that these attacks could be solved by telecom operators is over. The developments in the world show that a hybrid anti-ddos topology is needed for equipment that can make examination of DDOS package in details in own data centre of the corporation. At this point, corporations should complete their unfortunately delaying investments and establish hybrid (telecoms and their own data centre) DDOS security topology."

(/padphoto/49251892/22/afd23c93-a1c0-e311-b0d5-001a6465f174)