***PwC Türkiye***

Köşe Yazıları

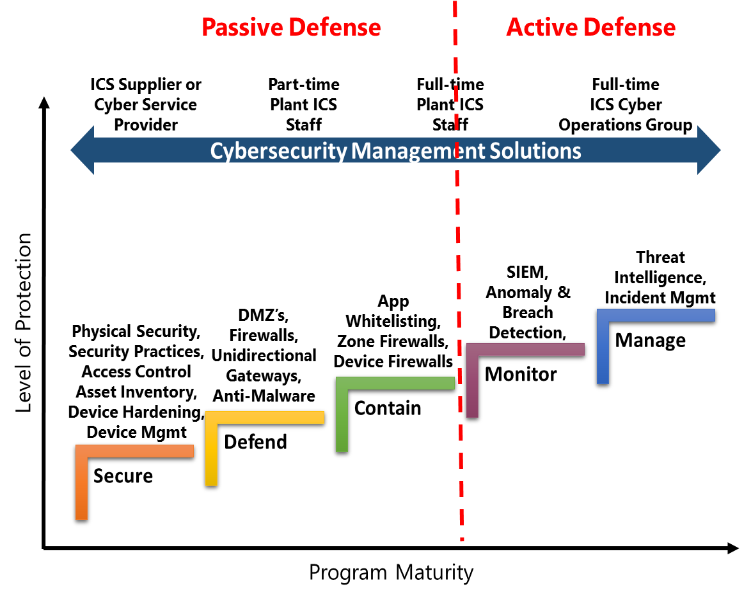
*Tarih:23.05.2021*

# [www.pwc.com.tr](http://www.pwc.com.tr/)

Siber Güvenlikte Aktif Savunma

Bu yazımızda “Aktif Savunma” ve genellikle karıştırılan “Karşı Sızma/Hackleme” kavramlarından bahsedilecektir.

Savunma konusunu aktif ve pasif olarak ayırabilmekteyiz. Kurumlarda kullanılan güvenlik duvarları, IPS/IDS gibi sistemlerin/yapıların bütününe “pasif güvenlik” denmekte. Aktif güvenlik ise pasif güvenliğin ardından güvenliği daha efektif sağlamak adına yapılan çalışmaları kapsamaktadır.



SIEM, Anomali algılama, istihbarat, olay müdahale gibi kavramlar aktif güvenliğin altında ele alınabilir. Aktif güvenliğin amacı kurumlardaki pasif güvenliğin yeterli olmaması üzerine, güvenliğin daha dinamik sağlanması ve saldırganlara karşı korunma stratejileri ile birlikte bu korunma başarısının artmasını sağlamaktır.

Kurumlar içinde kurulan “Olay Tespit ve Müdahale Ekipleri” veya hizmetleri, balküp(honeypot)leri, log toplama araçları, siber istihbarat çözümleri, belirli aralıklarla yapılan güvenlik testleri ve kırmızı takım çalışmaları gibi çeşitli işlerin tamamı kurumların güvenliğinin sağlanması adına büyük rol oynamaktadır.

Yapılan bu çalışmaların geri dönütlerinin uygulanması, bu süreçlerin izlenmesi, takip edilmesi gibi işler de

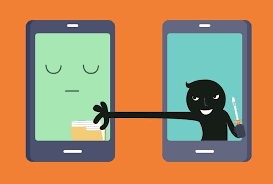
aktif savunmanın önemli adımlarındandır. Güvenliği genel olarak bir süreç olarak ele almamız gerektiğini düşündüğümüzde bu adımların birinin veya birkaçının atlanması kurum açıdan oluşabilecek riskleri artırabilmektedir. Aktif güvenliği, insan sağlığı gibi kurumsal güvenlik sağlığı olarak ele alabilmekte ve benzetebilmekteyiz. Sağlığımızı korumak adına yaptığımız şeyler nasıl süreklilik gerektiriyorsa

pasif güvenliğin yanında aktif güvenliğinde sıkı bir şekilde ilerletilmesi ve sürekliliğinin sağlanması gerekmektedir.

Kurumların çoğu günün sonunda “Aktif Savunma” kavramını yakından takip ediyor ve kullanıyor olsa da kavram olarak kimi zaman “Karşı Sızma/Hackleme” ile karıştırılmaktadır.

Saldırganlar sisteme sızmayı başardıktan ve fark edildikten sonra kurumlar bir karşılık vermek istemekte ve kimi zaman ne yapacakları konusunda fikirleri olmamaktadır.

 Hacklenen kurum kimi zaman bir şeyler yapmak istemekte ve ateşe ateşle karşılık vermeye çalışmaktadır. Burada “Karşı Sızma/Hackleme”den bahsedebilmekteyiz. Bu eylem fırlatılan bir füzeyi başka bir füze ile etkisiz hale getirmeye benzetilebilmekte. Burada yapılanın aslında bir angajman kuralına uygun olması gerektiği ve çoğu zaman bunun bir suç olduğunu belirtmemiz gerekir. Genel olarak karşıdan istihbarat toplamak, bu sızma eylemi yapanları tespit edebilmek, verilerin ne kadar çalındığını tespit etmek, kullanılan araçları veya yeni yöntemleri tespit edebilmek gibi amaçlar güdülebilmektedir.



Örnek olarak geçmiş zamanda bir ülkede gerçekleşen veri kaçırma eylemini bulmak için indirilen dosyalar içine gömülen bir zararlı verilebilir. Zararlı dosyayı da diğerleri ile birlikte açıp inceleyen ve kamera görüntüsü alınan saldırgan bu sayede yakalanabilmiştir.

“Aktif Savunma” ve “Karşı Hackleme/Sızma” konusundaki yaptırımlar ve hukuksal konular ise bağlı bulunan regülasyonlara, ülkelere ve ülkelerin politikalarına göre değişmektedir. Bu noktada yapılacak çalışmalar ilgili ülke veya regülasyon kurallarına göre yapılmak zorundadır.

Kurumların güvenliklerinin sağlanması ve sürdürülebilmesi için bu ve benzeri kavramların anlaşılması ve benimsenmesi önemlidir. Ayrıca hukuki tarafta da kurum için bir problem yaratmamak adına dikkatli davranmak, kurallara uymak gerekir.

***Berk KIRAS***

Cyber Security, Consultant

Email: berk.kiras@pwc.com

Referanslar ve Okuma Listesi

[1]-Fortigate - https://www.fortinet.com/resources/cyberglossary/active-defense

[2]-SANS <https://www.mitre.org/publications/technical-papers/active-defense-strategy-for-cyber>

[3]- ACSC - <https://www.cyber.gov.au/acsc/view-all-content/glossary/active-defence>

[4]-Aktif Siber Savunma ve Performans Analizi - <https://acikerisim.aku.edu.tr/xmlui/bitstream/handle/11630/6234/10066729.pdf>



© 2018 PwC Türkiye. Tüm hakları saklıdır. Bu belgede PwC ifadesi, PwC ağını veya PwC ağının üyesi olan bağımsız ve farklı tüzel kişiliklerden oluşan PwC Türkiye’yi ifade etmektedir. Daha detaylı bilgi için [www.pwc.com/structure](http://www.pwc.com/structure) adresini ziyaret edebilirsiniz.

Bu içerik sadece genel bilgi verme amacı taşır ve profesyonel danışmanlardan alınacak hizmetin yerine geçmez.