İstenmeyen Trafik (?)

Murat SOYSAL, Onur TEMİZSOYLU
TÜBİTAK ULAKBİM

Yaklaşık üç senedir istenmeyen trafik Akademik Bilişim ve benzer platformlarda tartışılmaktadır. Üniversitelerimizin ve araştırma kurumlarımızın çoğunun bu konuda UlakNet Kullanıcı Politikası'nıda sağlayan bir politikası oluşmamış durumdadır. İstenmeyen trafik, kaynakların tüketilmesi, kampüs içi ve hukuki şikayetlerin artması ile geçmişte olduğundan daha fazla soruna yol açmaktadır.

Üniversitelerin mevcut UlakNet bağlantıları, 2002 senesinde yeni UlakNet altyapısına geçilmesiyle yapılan iyileştirmelere rağmen hala Avrupa akademik ağına bağlı üniversitelerin bağlantı hızlarının çok altındadır. Kampüs içi omurgaların kullanıcıya sağladığı bant genişliklerinin UlakNet bağlantılarına göre daha iyi olması, UlakNet omurgasının dış bağlantılarından büyük boyutlu saldırıların çok sık gelebilmesi (Uzakdoğu ülkelerinden kaynaklı DDoS saldırıları, SPAM yayan virüsler gibi) bu bağlantıların kullanılamaz hale gelmesine yol açabilmektedir. Dolayısıyla UlakNet genelinde ve üniversiteler tarafında istenmeye trafik konusunda diğer ülkelere göre daha fazla çalışma yapılması gerekmektedir.

Üniversitelerde istenmeyen trafiğin engellenebilmesi konusundaki en büyük teknik eksiklik, trafiğin izlenmemesidir. Aşırı trafik yaratan kullanıcıların grafikler ve istatistik programları sayesinde belirlenmesi, SPAM trafiği için mail sunucu günlüklerinin incelenmesi bu çalışmalara örnek olarak verilebilir.

Bütün istenmeyen trafik tipleri için teknik çözümler bulunmaktadır. Bunların çoğu UlakNet içinde üniversiteler ve TÜBİTAK ULAKBİM tarafından kullanılmakta ve denenmektedir. P2P trafiğinin engellenmesi veya sınırlandırılması için IPP2P, Snort, NBAR, SPAM için SpamAssassin, virüs için Clam, Amavis ve ticari virüs tarayıcılar uygulanan çözümlerden bazılarıdır. Kalıcı ve etkisi hissedilebilir sonuçlar için tüm istenmeyen trafik tiplerine yönelik önlemler yukarıda bahsi geçen ve ya benzeri programlar yardımıyla alınmalıdır. Bununla birlikte istenmeyen trafiği yaratan sebeplerdeki hızlı değişim ve gelişimi takip edebilmek amacıyla www.securiteam.com, www.seclists.org gibi siteleri takip etmek gerekmektedir.

Alınan bu teknik önlemlerin tam anlamıyla başarılı olması için idari önlemlerle desteklenmesi gerekmektedir. İstenmeyen trafikle mücadelenin bir parçası olarak UlakNet'e bağlı her uçta oluşturulması gereken Kullanıcı Politikası bu idari önlemleri açıkca belirtmeli, böylece alınacak tedbir ve uygulanacak yaptırımların çerçevesini oluşturmalıdır. ULAKBIM Kullanım Politikası Sözleşmesiyle çelişmemesi gereken bu politikalar teknik önlemlere kılavuz olmanın yanı sıra motive edici bir unsur teşkil etmektedir.