

Bilgi Güvenliđinin Yönetimle İmtihanı

Bilgi güvenliđi yönetiminde aslında tüm yönetim sistemleri için geçerli klişe bir deyim vardır, yönetim desteđi olmazsa olmaz. Bu deyimi tamamlayıcı bir şey daha söylemek gerekirse; yönetim desteđi sadece bütçe sağlama ile sınırlı kalırsa yine olmaz. Etkili bir Bilgi Güvenliđi Yönetim Sistemi'nin (BGYS) ortaya konabilmesi için yönetimin bilgi güvenliđini stratejik bir gereklilik olarak ele alması gereklidir.

Diyelim ki bilgi güvenliđi bir kurum için gerçekten çok önemli, bu durumda yönetimin zaten buna destek sağlaması gerekmez mi? Sizin de tahmin edebileceđiniz gibi maalesef durum çođunlukla tersidir. Peki neden? Bunun iki temel sebebi vardır:

Birincisi bilgi güvenliđinin sunumunun genellikle "kötü" durumlarla ilgili oluşudur. Kim kötü şeyler duymak ister, geçmişteki olaylardan daha çok kötü olanlarını mı hatırlarız yoksa iyi olanlarını mı? İnsanlar kararlarının çođunu (sanıyorum pek çok insan tamamını) duygusal olarak verir. İnanmayanlar satışıçılara sorsun. Eğer yönetim desteđini alabilmek için felaket tellallıđı yaparsanız belki insanları şoktan şoka sokabilir herkesin dikkatini üzerinizde toplayabilirsiniz. Hatta o kadar iyi hazırlanabilirsiniz ki kurumunuzun başına gelmiş somut olayları, rakiplerinize dair yaptığınız güvenlik olay araştırmalarını profesyonelce sunabilirsiniz. Ancak bunları sunduđunuz insanlar gelirleri artırmaya, şirketi büyütmeye ve dolayısı ile kendi geleceklerini iyileştirmeye odaklanmış insanlar olacaktır. Bu konumda olan insanlar motivasyonlarını ayakta tutabilmek için iyimser olmak zorundadır. Bu dinleyicilere uygulayacađınız korku duşu yazık ki uzun süreli bir etkiye sahip olmayacaktır. İnsan doğası bu sonucu doğuracaktır.

İkinci sebep bilgi güvenliđi tehditlerinin bazılarının (fiziksel güvenlik, iş sürekliliđi gibi) herkes tarafından tahayyül edilebilecek olgular olması, ancak pek çok tehdidin konunun uzmanı olmayan kişilere çok karmaşık gelmesidir. Yine insan doğası geređi karmaşık konulara odaklanmak zordur, hele hele kişisel amaçlarımız ile pek de ilgisi yoksa.

Hal böyle iken bir yönetim toplantısında bilgi güvenliđine ilişkin iyi bir sunum yapan ve destek gördüğünü düşünen Bilgi Güvenliđi Yöneticisi (BGY) bir ay sonra arkasına döndüğünde kimseyi bulamazsa şaşırılmamalıdır. Yukarıda sayılan olumsuz olguları olumluya çevirmek ya da en azından etkilerini azaltmak için ne yapılabilir? Birinci konu ile ilgili olarak desteđi alınmak istenen tarafların hedeflerine paralel ifadeler kullanılmalıdır. Örneđin satış ve pazarlamadan sorumlu bir yöneticinin bulunduđu toplantıda bilgi güvenliđi ihlaline uğrarsak müşteri güvenini kaybedebilir ve satış kaybına uğrayabiliriz yerine, bilgi güvenliđi konusuna gereken önemi verirsek müşterinin güvenini kazanırız bu da orta uzun vadede piyasa oranımızı artırmamıza yardımcı olur, insan kaynakları yöneticisinin bulunduđu bir toplantıda sektörde bu konuda gerekli çalışmaları yaparsak çalışanlarımızın gözünde kurum deđeri artar, hatta kurumumuzdan ayrılan çalışanlar sonraki işyerlerinde bizde yapılan uygulamaları anlatır, finans ve mali işlerden sorumlu bir yöneticinin bulunduđu bir toplantıda kurumumuzun riski dolayısı ile belli konularda finansman maliyeti azalır, kurum deđerimiz artar, genel müdür ve riskten sorumlu yöneticilerin bulunduđu toplantılarda bir hizmet kesintisine uğradığımızda veya güvenlik ihlali gerçekleştiğinde durumu geređi gibi yönetebilirsek toplum nezdinde itibarımız yükselir gibi ifadeler kullanmak olumsuz ifadelerden daha çok destek sağlayacaktır.

İkinci konu, yani bilgi güvenliđi tehditlerinin karmaşıklıđı ile ilgili kolay bir yol olduğunu düşünmüyorum, en azından birinci konuyu halletmek kadar kolay deđildir. Bu alanı ele almak isteyen BGY'lerinin karmaşık tehditleri sıradan kişilerin anlayacađı biçimde ifade edebilecek kadar teknik yetkinliğe sahip olmaları gerekir. Bu konuyu halletmenin ikinci önemli adımı da iletişime önem verilmesidir. İletişimdeki başarı en az teknik yetkinlik kadar önemlidir. Özellikle kısıtlamaların arkasındaki gerekçelerin etkili iletişimi verilen desteđi artıracaktır.

© 2009 BTRisk. Tüm hakları saklıdır.