İhracatta pazar çeşitliliğinin önemi

ŞEFİKERGÖNÜL

Tek müşteriye çalışan bir işletme, fiyat güncellemesinde anlaşmazlık çıkması ve müşterinin **sipariş vermemesi** üzerine **bir anda** duvara çarpmış gibi **durdu**. Maddi durumlarının iyi olmasına güvenerek "**Dayanırız ve yeni müşteri buluruz**" diyordu. Ancak hazıra dağ dayanmaz özdeyişi de orada duruyor.

Ayrıca "**Yumurtaların hepsini aynı sepete koymayın** " özdeyişi duyulmamış mıydı?

Başka bir dostumuza ihracat çalışmalarının nasıl gittiğini sorduğumda, "**Hocam iyi bir müşterim var"** diyerek, başka bir yere bakmayı düşünmediğini söylemişti.

Aradan geçen epey bir zaman sonra telaşla beni aramıştı. Heyecanının nedenini sorduğumda **"Müşteri ödememi ciddi boyutta kesmiş"** diyerek olayın detayını anlattı.

Müşterisinin yeni muhasebecisinin uluslararası ticaretteki eksik bilgisi nedeniyle yanlış bir uygulama yapılmıştı. Açıklama yolladık, düzeltme yaptırdık ve paranın tamamı geldi.

Çözüm sonrası arkadaşımıza sordum **"Tek müşteriyle çalışmanın sakıncasını anlatıp hem pazar hem de müşteri çeşitlendirmesini salık vermiştim hatırladın mı?"**

Bir başka dostumuz da müşterisine ciddi boyutta ihracat yapıyor ve o arada kendisine gelen başka yabancı bir müşterisine de küçük bir miktar ürün tedarik ediyordu.

O da bir gün arayıp acilen görüşmek istediğini söyledi.

Almanya'daki büyük müşterisi batmış ve kayyum tayin edilecekmiş.

Telaşının arkasındaki neden de bu müşteride epeyce bir alacağı birikmiş olması.

Uzun süren çabalarımız sonucunda ve biraz eziyetli olsa da alacaklarının önemli bir kısmının tahsilatı sağlandı.

Bu dostumuz da farklı pazarlara, ihracat yapılan ülke ve müşteri sayısının artırılmasına çok sıcak bakmıyordu. Artan ihracatın hem operasyonel işlerin hem de dış ticaret elemanı artışına neden olacağı ve bunun da fazladan masraf çıkaracağı gibi tuhaf bir düşüncesi vardı.

Ancak bu olaydan ders almış olsa ki bir süre sonra dış ticaret ekibini artırmıştı.

Daha sonra da ekibin başındaki arkadaş beni arayıp Güney Amerika'ya gideceğini söyleyerek tavsiye istediğinde, hayretle gülmekten bu arkadaşımıza cevap verememiştim.

Bu üç örnek de yaşanmış olaylardır...

Eskiler kıssadan hisse çıkartın derler ya bizler de öyle yapalım ve bu hikâyelerden ders çıkartalım.

İster iç piyasa isterse ihracat piyasası olsun bir müşteriye bağımlı olmanın sakıncalarını tekrar etmeye gerek var mı bilmem ama özellikle ihracatta buna fazlaca rastlıyoruz.

Son yıllarda Türk ihracatçısının açılmadığı pazar kalmadı gibi diyebilsek de pazar çeşitlendirmesine giden ihracatçı sayımız kaç tane acaba?

Bunun nedenine inmek için **"Neden pazar çeşitlendirmesine gidemiyoruz"** diye sorsak mı?

Bu sorunun cevabı olarak, **"İhracatçımız ağırlıklı olarak kendisine gelen müşterinin taleplerini karşılıyor"** diyebiliriz. Hal böyle olunca da ihracat yaptığımız ülke ve yabancı alıcı sayımız bize erişim sağlayanlarla kısıtlı kalıyor.

Kısıtlı pazar ve kısıtlı müşteri sayısından sıyrılmak istiyorsak yapılması gerekenler belli...

Pazar araştırmasına önem vererek önce **hedef ülke/pazar** belirlemeye çalışmalıyız.

Sonra da o hedef pazarlarda **potansiyel müşteri araştırmasına** gitmek, bizleri hem müşteri özelinde hem de ülkeler genelinde bizleri **risklerden uzaklaştıracaktır**.

İhracatta doğru strateji, pazar çeşitliliği ve istikrar üzerine kurulmalıdır. Dış satımda riskin azalması, öngörülebilirliğin artması bu iki olgudaki başarıyla sağlanır.

Ne kadar çok farklı ülkede ve ne kadar fazla sayıda ihracat müşterisine ürün satabiliyorsak güvencemiz de o kadar güçlü olacaktır.

Tek ülke, hem politik hem de ekonomik riskimizi yüksek seviyede tutar.

Tek veya bir adet çok büyük müşteri de finansal riskimizi artırır.

Hedef pazar belirleme konusunda en önemli kaynağımız www.trademap.org ki bu portaldan nasıl fayda sağlayacağımız hakkında YouTube üzerinde sayısız video bulabilirsiniz.

Öte yandan Ticaret Bakanlığı'nın sitesi her geçen gün ihracatçılarımız için daha fazla bilgi desteği sağlar bir duruma geliyor.

İhracatçılarımızın hem pazar araştırması yapmakta kullanabilecekleri hem de ihracatçıya verilen devlet desteklerini öğrenebilecekleri https://kolaydestek.gov.tr/ ve https://www.kolayihracat.gov.tr/ gibi sayfalar bakanlık sitesinde yer alıyor.

Ayrıca hedef ülke seçiminde ve seçilen hedef ülkelere ait değerlendirmelerde kullanabileceğimiz verileri bulabileceğimiz https://www.cia.gov/the-world-factbook/ sitesi bizlere çok değerli bilgileri sunuyor. Burayı kullanarak ürün/pazar eşleştirmesi çalışmalarını rahatlıkla yapabiliriz.

Hedef ülkelerin ülkemizin ve rakip ülkelerin ürünlerine uyguladığı gümrük vergilerini https://www.macmap.org/ adresinde bulabilir ve kıyaslama yapabiliriz. İnternetin gücüne karşın fuarlar ise hala önemini koruyor. Fuarlar konusunda önemli bir kaynak olarak https://ticaret.gov.tr/ihracat/fuarlar sayfasını önerebilirim.

Tohum ekmezseniz hasat yapamazsınız...

İhracat için yatırım gerekir.

İşletmenizin üretiminin ihracat yapmaya hazır olduğunu varsayarsak bu yatırımların en önemlisi de pazar ve müşteri bulmak için yapılacak olandır.

Masa başı araştırmalar masrafsız olduğu kadar etkisi de azdır.

Bizlere öngörü ve planlama yapabilmemiz için veri sağlar.

Ancak hedef ülkeye giderek orada yapılacak çalışmalarla kurulacak temasların faydası tartışılmaz.

Unutmayalım gözden ırak olan gönülden de ırak olurmuş.

DİJİTALLEŞMENİN VAZGEÇİLMEZ KURALI

Siber güvenlik nasıl sağlanır?

HİLMİ DEVELİ

Dijital dönüşüm fırtınasının yaşandığı veri çağında, kamudan özel sektöre; küçük ölçekli işletmelerden büyük ölçekli işletmelere, kurum, kuruluşlara, bireylere, ülkelere kadar her alanda ve her yerde siber saldırıları, veri ihlallerini, siber suçlar gibi tehditleri, zaman, verimlilik, para, itibar kaybını önlemek büyük önem taşıyor. Riskleri minimize etmek; bilgi güvenliğini sağlamak, dijital varlıkları korumak her zamankinden daha değerli. Günümüzde fabrikalardan, akıllı fabrikalara, akıllı ofislerden, akıllı binalara, akıllı şehirlere, hastanelerden, okullara, trafiğe, evlerden, ev ve ofis eşyalarına (akıllı televizyonlar, akıllı bulaşık ve çamaşır makineleri, temizlik robotları vs.), arabalara, araçlara, elimizdeki tüm mobil ve akıllı cihazlara (akıllı telefon, tablet, dizüstü bilgisayar, giyilebilir cihazlar vs.), otonom araçlara kadar her yerde kullanılan yapay zeka aynı zamanda siber saldırıların açık hedefi.

Nedir bu fidye yazılımı?

Siber saldırılardan fidye amaçlı yazılımlar günümüzde kurban olarak hedefledikleri işletmeler ya da kişilerin canını yakıyor. Fidyeci (CryptoLocker) kullanıcılardan dosyaları şifrelemek yoluyla para talep etmeye dayalı zararlı bir yazılımdır.Ransomware Fidye yazılımı, fidye ödenene kadar kritik veri veya sistemlere erişimi yok ederek ya da engelleyerek kurbanı tehdit eden bir tür kötü amaçlı yazılımdır. Fidye yazılımı saldırıları, para talep etme aracı olarak bir kişinin veya kurumun verilerinin ya da cihazlarının kontrolünü ele geçirmeye dayanır. Etkilenen verilerin şifresinin çözülmesi ve mağdura erişimin geri verilmesinden önce ödeme talep edilir.

Dijitalleşme, iş planlarında ana gündem. Bu konuda bilgi sahibi olmayan hatta harekete geçmeyen yok gibi. Peki, dijitalleşmenin altın kurallarından siber güvenlik, şirketlerin ne kadar gündeminde? Bu soruya da son dönemdeki gelişmelere bakarak olumlu yaklaşım getirmek mümkün. Siber riskler konusu, en başta da fidye yazılımlarındaki gelişmeler, şirketlerin gündemlerindeki ağırlığını uzun süre devam ettirecek.

Fidye yazılımı;
- ► Sosyal mühendislik fidye yazılımı
- ► İnsan tarafından yürütülen fidye yazılımı

olarak gruplandırılır.

Sosyal mühendislik fidye yazılımı

Bu saldırılar, kurbanı bir bağlantıya tıklaması veya cihazlarına fidye yazılımı yükleyecek bir e-posta ekini açması için kandırmak üzere saldırganın meşru bir şirket veya web sitesi gibi davrandığı bir aldatma biçimi olan kimlik avını kullanır. Saldırılar genellikle kurbanı korkudan hareket etmeye yönlendiren uyarı mesajları içerir. Örneğin, bir siber suçlu tanınmış bir marka gibi davranabilir ve birisine şüpheli etkinlik nedeniyle hesabının dondurulduğunu bildiren bir e-posta göndererek bu kişiyi sorunu çözmek için e-postadaki bir bağlantıya tıklamaya teşvik edebilir. Bağlantıya tıkladıklarında fidye yazılımı yüklenir.

İnsan tarafından yürütülen fidye yazılımı

Genelde çalıntı hesap kimlik bilgileri ile başlar. Saldırganlar bu şekilde bir kurumun ağına erişim elde ettikten sonra, daha geniş erişim kapsamına sahip hesapların kimlik bilgilerini belirlemek için çalınan hesabı kullanarak yüksek finansal getiri potansiyeli olan veri ve iş açısından kritik sistemleri ararlar. Daha sonra, örneğin hassas dosyaları şifreleyerek bu hassas verilere veya iş açısından kritik sistemlere fidye yazılımı yüklerler, böylece kuruluş bir fidye ödeyene kadar bunlara erişemez. Siber suçlular, anonim olması nedeniyle bir kripto para biriminde ödeme talep etme eğilimindedir.

Fidye yazılımı iki ana biçimde gelir:

- ►Kripto fidye yazılımı,
- ►Kilitleme fidye yazılımı.

Kripto fidye yazılımı

Bir kişi veya kurum bir kripto fidye yazılımı saldırısının kurbanı olduğunda, saldırgan kurbanın hassas verilerini veya dosyalarını şifreler, böylece istenen fidyeyi ödemedikçe bunlara erişemezler.

Teorik olarak, kurban ödeme yaptığında, dosyalara veya verilere erişmek için bir şifreleme anahtarı alır.

Ancak bir kurban fidyeyi ödese bile, siber suçlunun şifreleme anahtarını göndereceğinin veya kontrolü bırakacağının garantisi yoktur.

Doxware, genellikle kurbanı küçük düşürmek veya fidye ödemeleri için utandırmak amacıyla, bir kurbanın kişisel bilgilerini herkese açık olarak ifşa etmekle tehdit eden ve şifreleyen bir kripto fidye yazılımı biçimidir.

Kilitleme fidye yazılımı

Kilitleme fidye yazılımı saldırısında, kurbanın cihazı kilitlenir ve oturum açamaz. Kurbana ekranda kilitlendiklerini belirten ve erişimi yeniden kazanmak için nasıl fidye ödeyeceğine ilişkin talimatları içeren bir fidye notu gösterilir. Bu fidye yazılımı türü genellikle şifreleme içermez, bu nedenle kurban cihazına yeniden erişim sağladığında tüm hassas dosyalar ve veriler korunur.

Şirketler tedbirleri ciddiyetle ele almalı

Fidye yazılımı saldırıları çok farklı şekillerde karşımıza çıkabilir ve saldırının boyutları çok farklı olabilir. Saldırı vektörü, kullanılan fidye yazılımı türleri için önemli bir faktördür.

Saldırının büyüklüğünü ve kapsamını tahmin etmek için hangi verilerin silineceğini veya yayınlanabileceğini her zaman dikkate almak gerekir.

Fidye yazılımı türü ne olursa olsun, önceden verileri yedeklemek ve güvenlik yazılımları kullanmak, bir saldırının etkisini ciddi ölçüde azaltabilir.

"Siber güvenlik okuryazarlığı artıyor"

ISR Bilgi Güvenliği şirketi Kurucu Ortağı ve Genel Müdürü Eren Ertem Develi, fidye saldırıları, donanım arızası veya operasyonel hata gibi sebepler sonucunda verinin sahipliğinin veya veri kaybının oluşması durumuna karşı pek çok işletmenin önlemlerini almakta olduğunu söyledi.

Eren Ertem Develi, konuya ilişkin görüşlerini şu şekilde dile getirdi:

"Bu önlemler veriyi işleyen işletme açısından yeterli görünse de artık verisi çalınan bireyler veya işletmeler açısından da sorumluluklar mevcut. Operasyonlarını yüksek düzeyde dijital kaynaklar üzerinde yürüten işletmelerimizde, erişimin yüksek tutulması gereken dijital kaynaklarda, rekabetin yüksek, müşteri kaybının da telafi edilemez düzeyde önemli olduğu sektörlerde, güvenlik önlemlerinin bu önem doğrultusunda alınmasının cironun korunabilmesi ve orta vadede ise artması açısından önem taşıdığını belirtmek gerekir. KOBİ işletmelerimizin de giderek artan dijital kaynak kullanımlarını düşündüğümüzde, farkındalıklarını artırmalarını ve çalışmaların bu bilgiler eşliğinde kuvvetlendirilmesini öneririz".