KULLANIM SENARYOSU

NextCloud EFSS içerisinde depolanan hassas verilerin şifrelenerek saklanması

Problem

NextCloud ağ üzerinden gelişmiş dosya transferi ve paylaşımına izin veren özelliklere sahip, açık kaynak kodlu ve ücretsiz bir Kurumsal Dosya Senkronizasyonu ve Paylaşımı (EFSS) yazılımıdır. Verilerini depolamak için bir bulut sistemine ihtiyacı duyan ancak Google, Dropbox, vb. kamuya açık servis sağlayıcılara güvenmek istemeyen tüm firmalar NextCloud yazılım paketini kendi sunucularına kurarak çalışanlarına kullandırabilirler.

Savunma alanında hizmet veren özel bir firma resmi evraklar ve proje dosyaları dahil tüm önemli belgelerini, veri yönetimini sınırlayan geleneksel Ağ Dosya Sisteminden, birlikte çalışmayı kolaylaştıran yeni nesil bir yapıya aktarmak için kendi bünyesinde NextCloud kurulumu gerçekleştirmiştir. NextCloud yazılımında her ne kadar sunucu ile istemciler arasındaki veriler ağ üzerinde şifrelenerek güvenli bir şekilde taşınsa da sunucu üzerindeki veriler şifresiz olarak saklanmaktadır. Yazılımın sağladığı erişim denetimi son kullanıcılar için geçerli olup başta Bilgi Teknolojileri (BT) yöneticisi olmak üzere sunucuya erişen herkes depolama alanındaki dosyaların içeriğini görüntüleyebilir. Bu durum KVKK başta olmak üzere firmanın tabi olduğu Yasal Mevzuat ve yürürlükte olan Firma Bilgi Güvenliği Politikasına aykırılık teşkil etmektedir.

Çözüm

KRYPTOS kullanılarak çalışan bilgisayarında bulunan dosyalar, NextCloud istemcisi tarafından NextCloud sunucusuna senkronize edilmeden önce, her bir çalışan için özel olarak kişiselleştirilmiş Token içerisindeki anahtarlar ile şifrelenir. Bu sayede KRYPTOS dosya konumundan bağımsız olarak uçtan uca şifreleme sağlamış olur. NextCloud sunucusunda bulunan dosyalar insan hatası sonucu ifşa olmaz ya da kötü niyetli kişiler tarafından sızdırılamaz.

KRYPTOS ile klasörlere erişim denetimini son kullanıcılar kendileri yöneterek ilgili kişileri ya da grupları yetkilendirebileceği gibi firma politikasına bağlı olarak bu yönetim BT'ye de bırakılabilir.

YÖNETİCİ ÖZETİ

Kısa Özet

Endüstri : Savunma Sanayi

Kurum : Savunma Sanayiinde faaliyet gösteren özel bir firma

Mevcut Zorluk

1. NextCloud depolama biriminde belgelerin şifresiz olarak saklanması
2. Sadece yetkili personelin erişiminin 2FA ile garanti edilmesi
3. Şifrelemenin getirdiği verimsizlik ve süreçlerin insan hatasına açık olması
4. KVKK başta olmak üzere yasal mevzuata uyum

Sonuç

1. NextCloud depolama biriminde tüm belgeler eşsiz birer anahtarla şifrelenmiş olarak saklanmaktadır
2. Belgelere sadece yetkili kişiler erişebilmektedir
3. KRYPTOS SafeBox ile kullanım kolaylığı sağlanmış ve verimsizliğini önüne geçilmiştir
4. KVKK başta olmak üzere yasal mevzuata uyum sağlanmıştır

Erişim yönetimini BT yapsa dahi KRYPTOS içerisinde bulunan görevler ayrılığı ilkesi gereği BT yöneticileri kendilerini bir şifreleme grubuna ekleyemezler. KRYPTOS kullanmanın bir diğer avantajı NextCloud tarafından sağlanan Senkronizasyon Klasörü istemcisiyle yapılan entegrasyondur. Bu entegrasyon sayesinde çalışanlar NextCloud Senkronizasyon Klasörü ile benzer şekilde çalışan Kryptos SafeBox modülüyle günlük iş yapış şekillerini değiştirmeden her zaman şifreli olarak saklanan dosyalar ile verimli bir şekilde çalışırlar.

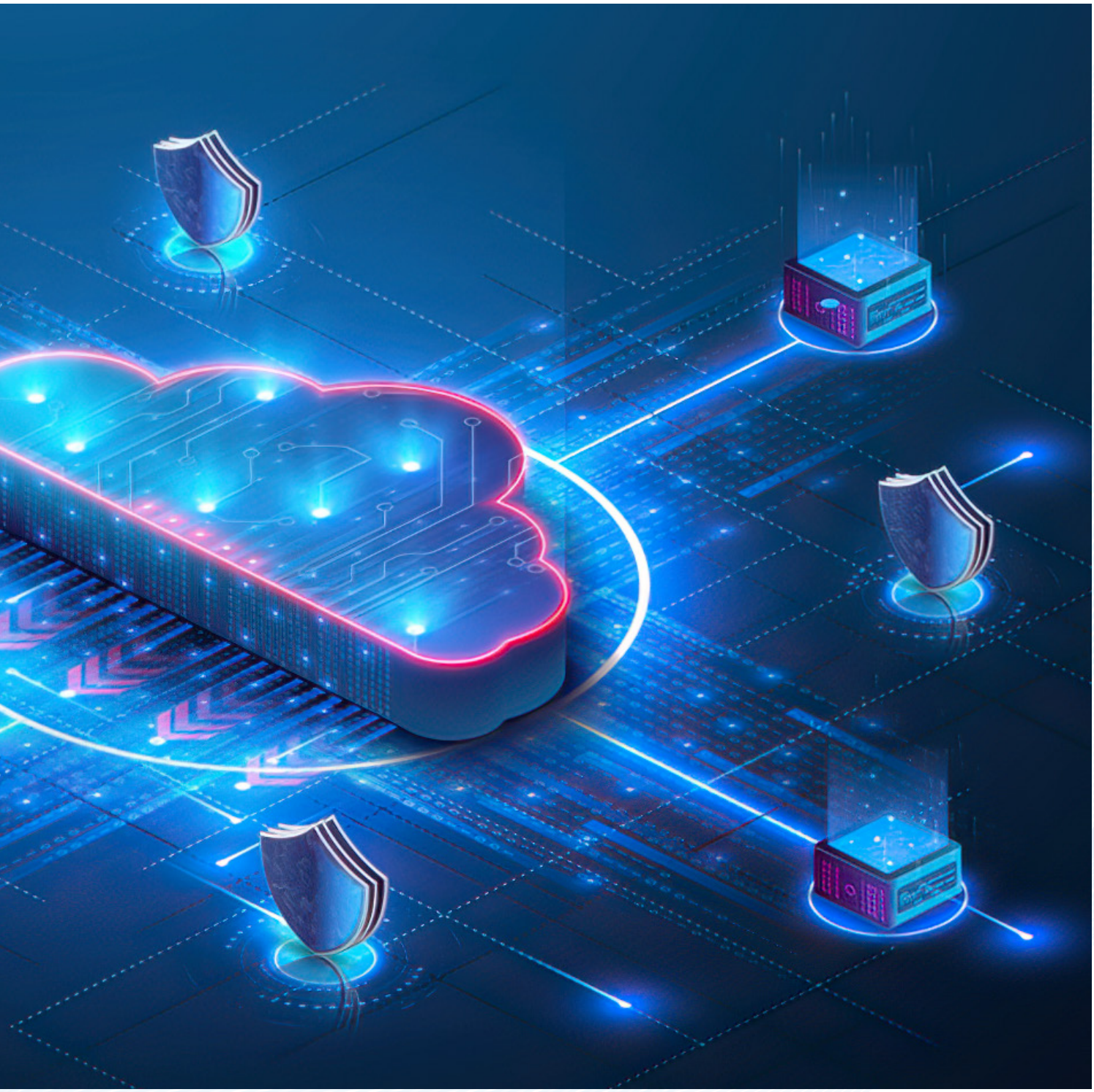
Sonuçlar

- Savunma Sektöründe faaliyet gösteren özel bir firma resmi evraklar ve proje dosyaları dahil tüm belgelerini çalışanların iş süreçlerini ve bu süreçlerdeki dosya erişimlerini kolaylaştırmak için Bulut tabanlı bir yapıya taşımak istemiştir. Bu amaçla açık kaynak kodlu ve ücretsiz bir Kurumsal Dosya Senkronizasyonu ve Paylaşımı platformu olan NextCloud tercih edilmiş ve firma kendi veri merkezinde özel bir NextCloud kurulumu gerçekleştirmiştir. Uç birimlere kurulan NextCloud istemcisi sayesinde çalışanlar Yerel Senkronizasyon Klasörleri üzerinden dosyalara erişim sağlarken, tüm dosyalar firmanın kendi veri merkezinde bulunan NextCloud sunucusunun depolama birimine senkronize edilerek saklanmaktadır.
- Bu noktada firmanın tabi olduğu yasal mevzuat ve uygulamakta olduğu Bilgi Güvenliği Politikası gereği NextCloud sunucusunda depolanan dosyaların şifrelenmesi ve şifreli dosyaları sadece yetkisi olan çalışanların görebilmesi ve bu dosyalar üzerinde çalışabilmesi ihtiyacı ortaya çıkmıştır.
- KRYPTOS dosya konumu, türü ve boyutundan bağımsız çalışan, endüstri standardı şifreleme algoritmaları ve teknikleri kullanarak uçtan uca şifreleme sağlayan bir çözümdür. Şifreleme işlemleri her çalışan için özel olarak kişiselleştirilmiş Token kullanılarak yapılmaktadır. Bu Token vasıtasıyla İki Faktörlü Doğrulama (2FA) yanında şifreleme ve şifre çözme işlemleri de Token'a aktarılarak yüksek güvenlik sağlanmaktadır.

- KRYPTOS aynı zamanda şifreli dosyalar ile kolay, hızlı ve güvenli bir şekilde işlem yapılmasına olanak verir. NextCloud sunucusunun depolama biriminde şifreli olarak saklanan dosyalar, NextCloud istemcisi tarafından, çalışan uç birimindeki Yerel Senkronizasyon klasörüne yine şifreli olarak kaydedilir. KRYPTOS kullanan çalışanlar diskte her zaman şifreli olarak saklanan bu dosyalar ile şifresizmiş gibi işlem yapabilmektedir; yani herhangi bir dosyayı açıp,

Özet

- Firmanın kendi veri merkezinde bulunan sunuculara kurduğu NextCloud EFSS üstünde bulunan dosyalar şifrelenerek sadece yetkili personelin KRYPTOS üzerinden bunlara erişebilmeleri sağlanmıştır.



KRYPTOS
BULUT ORTAMLARINDAKİ
VERİLERİNİZ İÇİN TAM BİR
KORUMA SAĞLAR.

CUSTOS™
SOLUTIONS

Teknopark İstanbul 1. Blok Kat 2, Pendik, İstanbul / TURKEY
T : +90 850 480 77 44 | +90 216 290 52 86

www.custossolutions.com