Botium Toys: Kapsam, hedefler ve risk değerlendirme raporu

Denetimin kapsamı ve hedefleri

Kapsam: Kapsam, Botium Oyuncak'ta tüm güvenlik programı olarak tanımlanır. Bu, tüm varlıkların, kontrollerin ve en iyi uyumluluk uygulamalarının uygulanmasıyla ilgili dahili süreçler ve prosedürlerle birlikte değerlendirilmesi gerektiği anlamına gelir.

Hedefler: Botium Toys'un güvenlik duruşunu iyileştirmek için hangi kontrollerin ve uyumluluk en iyi uygulamalarının uygulanması gerektiğini belirlemek için mevcut varlıkları değerlendirin ve kontrolleri ve uyumluluk kontrol listesini tamamlayın.

Dönen varlıklar

BT Departmanı tarafından yönetilen varlıklar şunları içerir:

- Ofis içi iş ihtiyaçları için şirket içi ekipman
- Çalışan ekipmanı: son kullanıcı cihazları (masaüstü bilgisayarlar/dizüstü bilgisayarlar, akıllı telefonlar), uzak iş istasyonları, kulaklıklar, kablolar, klavyeler, fareler, yerleştirme istasyonları, güvenlik kameraları vb.
- Yerinde ve çevrimiçi olarak perakende satışa sunulan vitrin ürünleri; Şirketin bitişiğindeki depoda saklanır
- Sistem, yazılım ve hizmetlerin yönetimi: muhasebe, telekomünikasyon, veritabanı, güvenlik, e-ticaret ve envanter yönetimi
- İnternet erişimi
- Dahili ağ
- Veri saklama ve depolama
- Eski sistem bakımı: insan tarafından izlenmesi gereken kullanım ömrü sona eren sistemler

Risk değerlendirmesi

Risk açıklaması

Şu anda, varlıkların yönetimi yetersiz bir şekilde yürütülmektedir. Ek olarak, Botium Toys tüm uygun kontrollere sahip değildir ve ABD ve uluslararası düzenlemeler ve standartlarla tam olarak uyumlu olmayabilir.

En iyi uygulamaları kontrol edin

NIST CSF'nin beş işlevinden ilki Tanımla'dır. Botium Toys'un varlıkları uygun şekilde yönetebilmeleri için tanımlamaya yönelik kaynakları ayırması gerekecektir. Ek olarak, mevcut varlıkları sınıflandırmaları ve sistemler de dahil olmak üzere mevcut varlıkların kaybının iş sürekliliği üzerindeki etkisini belirlemeleri gerekecektir.

Risk puanı

1'den 10'a kadar bir ölçekte, risk puanı 8'dir ve bu oldukça yüksektir. Bunun nedeni, kontrol eksikliği ve en iyi uyumluluk uygulamalarına bağlılıktır.

Ek açıklamalar

Bir varlığın kaybından kaynaklanan potansiyel etki orta olarak derecelendirilir, çünkü BT departmanı hangi varlıkların risk altında olacağını bilmez. Botium Toys gerekli tüm kontrollere sahip olmadığından ve kritik verileri özel/güvende tutan uyumluluk düzenlemeleriyle ilgili en iyi uygulamalara tam olarak uymadığından, yönetim organlarından gelen varlıklara veya para cezalarına yönelik risk yüksektir. Belirli ayrıntılar için aşağıdaki madde işaretlerini gözden geçirin:

- Şu anda, tüm Botium Toys çalışanları dahili olarak depolanan verilere erişebilir ve kart sahibi verilerine ve müşterilerin PII/SPII'lerine erişebilir.
- Şifreleme şu anda müşterilerin şirketin dahili veritabanında yerel olarak kabul edilen, işlenen, iletilen ve saklanan kredi kartı bilgilerinin gizliliğini sağlamak için kullanılmamaktadır.
- En az ayrıcalık ve görev ayrımı ile ilgili erişim kontrolleri uygulanmamıştır.
- BT departmanı, veri bütünlüğünü sağlamak için kullanılabilirliği ve entegre kontrolleri sağlamıştır.
- BT departmanı, uygun şekilde tanımlanmış bir dizi güvenlik kuralına dayalı olarak trafiği engelleyen bir güvenlik duvarına sahiptir.
- Antivirüs yazılımı, BT departmanı tarafından düzenli olarak kurulur ve izlenir.
- BT departmanı bir izinsiz giriş tespit sistemi (IDS) kurmadı.

- Şu anda yürürlükte olan herhangi bir felaket kurtarma planı yoktur ve şirket kritik verilerin yedeğine sahip değildir.
- BT departmanı, bir güvenlik ihlali olması durumunda AB müşterilerini 72 saat içinde bilgilendirmek için bir plan oluşturdu. Ek olarak, verileri uygun şekilde belgelemek ve sürdürmek için BT departmanı üyeleri/diğer çalışanlar arasında gizlilik politikaları, prosedürleri ve süreçleri geliştirilmiş ve uygulanmıştır.
- Bir parola politikası mevcut olmasına rağmen, gereksinimleri nominaldir ve mevcut minimum parola karmaşıklığı gereksinimleriyle uyumlu değildir (örneğin, en az sekiz karakter, harflerin ve en az bir sayının bir kombinasyonu; özel karakterler).
- Parola politikasının minimum gereksinimlerini uygulayan merkezi bir parola yönetim sistemi yoktur, bu da bazen çalışanlar/satıcılar bir parolayı kurtarmak veya sıfırlamak için BT departmanına bir bilet gönderdiğinde üretkenliği etkiler.
- Eski sistemler izlenir ve bakımı yapılırken, bu görevler için düzenli bir program yoktur ve müdahale yöntemleri belirsizdir.
- Botium Toys'un ana ofislerini, mağaza cephesini ve ürün deposunu içeren mağazanın fiziksel konumu, yeterli kilitlere, güncel kapalı devre televizyon (CCTV) gözetimine ve ayrıca işleyen yangın algılama ve önleme sistemlerine sahiptir.