ÖZET

SİBER SAVUNMA MERKEZLERİNDE VAKA BİLDİRİMİ SAĞLAYAN BİR SİSTEM

Bu buluş, siber savunma merkezinin karşılaştığı siber tehditlerin ilgili harici kaynaklara bildirilmesini sağlayan bir sistem (1) ile ilgilidir.

İSTEMLER

1. Siber savunma merkezinin karşılaştığı siber tehditlerin ilgili harici kaynaklara bildirilmesini sağlayan;
   - siber saldırılara ilişkin verileri depolamak üzere yapılandırılan en az bir vaka veri depolama modülü (2) içeren ve
   - üzerinde en az bir uygulama çalıştırmak üzere yapılandırılan en az bir elektronik cihaz (3)
   - elektronik cihaz (3) üzerinde çalışmak ve vakaya ilişkin sorguları vaka veri depolama modülüne (2) erişerek cevaplamak üzere yapılandırılan en az bir vaka sorgulama mobil uygulaması (4) ile karakterize edilen bir sistem (1).

2. Vaka müdahale süreçlerine dahil olan tüm vakalara ilişkin verileri depolamak üzere yapılandırılan vaka veri depolama modülü (2) ile karakterize edilen İstem 1'deki gibi bir sistem (1).

3. Vakalara ilişkin verileri önceden belirlenmiş şifreleme yöntemleri doğrultusunda şifreleyerek depolamak üzere yapılandırılan vaka veri depolama modülü (2) ile karakterize edilen İstem 1 veya 2'deki gibi bir sistem (1).

4. Firma çalışanı, firma direktörü gibi siber savunma yetkilisi kullanıcıların kullandığı ve üzerinde en az bir uygulama çalıştırmak üzere yapılandırılan elektronik cihaz (3) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

5. Elektronik cihaz (3) üzerinde çalışmak ve yetkili kullanıcının vakaya ilişkin sorgu yapmasını mümkün kılmak üzere yapılandırılan en az bir arayüz içermek üzere yapılandırılan vaka sorgulama mobil uygulaması (4) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

6. Vaka veri depolama modülüne (2) erişerek yeni vaka kaydı gerçekleştiğinde yetkili kullanıcıya bildirim göndermek üzere yapılandırılan vaka sorgulama mobil uygulaması (4) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

7. Yetkili kullanıcının mevcut vakalara ilişkin bilgi istemesini, sorgu yapmasını mümkün kılmak üzere yapılandırılan vaka sorgulama mobil uygulaması (4) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

8. Vaka veri depolama modülünde (2) şifrelenmiş biçimde depolanan vaka kayıtlarına ilişkin sorgu yapıldığında erişim izni olan yetkili kullanıcılara şifrelenmiş vaka kaydını iletmek üzere yapılandırılan vaka sorgulama mobil uygulaması (4) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

9. Vaka kaydının okunabilir olmasını sağlayan şifreyi yetkili kullanıcıya iletmek üzere yapılandırılan vaka sorgulama mobil uygulaması (4) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

10. Şifreyi açan yetkili kullanıcının vaka kaydını görüntülemesini mümkün kılmak üzere yapılandırılan vaka sorgulama mobil uygulaması (4) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

11. Sorgu sonuçlarını bir rapor biçiminde yetkili kullanıcının önceden tanımlanmış olan e-posta adresine göndermek üzere yapılandırılan vaka sorgulama mobil uygulaması (4) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (1).

12. Yetkili kullanıcıya raporu görüntülenebilir kılan bir şifre göndermek üzere yapılandırılan vaka sorgulama mobil uygulaması (4) ile karakterize edilen İstem 11'deki gibi bir sistem (1).

TARİFNAME

SİBER SAVUNMA MERKEZLERİNDE VAKA BİLDİRİMİ SAĞLAYAN BİR SİSTEM

Teknik Alan

Bu buluş, siber savunma merkezinin karşılaştığı siber tehditlerin ilgili harici kaynaklara bildirilmesini sağlayan bir sistem ile ilgilidir.

Önceki Teknik

Günümüzde firmalar siber savunma merkezlerinde bir vakayla karşılaştıklarında vakaya anında müdahale etmek ve gerekli incelemeyi yapmak durumundadır. Bu incelemeler esnasında firmalardan bilgi bekleyen diğer ekiplere ve vakaya dahil olmuş çalışanlara bilgi sağlanması gerekmektedir. Mevcut teknikte vakaların ilgili kişilere/birimlere bildirilmesi e-posta aracılığıyla gerçekleştirilmektedir. E-posta ile bilgi akışı sağlanırken incelemeler gecikmekte, efor harcanmakta ve yetkililerin vakaya ilişkin bilgilendirilmesi vakit almaktadır.

Mevcut teknikte bulunan çalışmalar göz önünde bulundurulduğunda vaka bildiriminde gereken eforun en aza indirilmesini ve vakaya ilişkin bildirimlerin anlık olarak yapılmasını sağlayan bir sisteme ihtiyaç duyulduğu anlaşılmaktadır.

Tekniğin bilinen durumunda yer alan US9697352 sayılı Birleşik Devletler patent dokümanında, siber savunma merkezinin siber tehdit olaylarını derleyen ve analistlere ileten, analistlerin çözmekte olduğu olaylarla ilgili harici kaynakları bilgilendirebilen bir sistemden bahsedilmektedir. Şirket içerisindeki siber savunma merkezi dahilinde hafıza elemanlı bir olay tepki birimi bulunmaktadır. Olay tepki birimi siber saldırı olaylarını ve olayla ilgili veriyi almakta, olayın ve verinin derlenmesini sağlamakta ve siber savunma analistlerine raporlanan siber saldırı

olaylarını ileterek çözümlenmesini sağlamaktadır. Olay tepki birimi ile iletişim halinde olan ve şirket personelinin mobil cihazlarında bulunan siber savunma uygulaması, ilgili olayın şifrelenmiş verilerine ve vaka raporlarına erişim sağlamaktadır. Yetkili şirket personeli, bildirdikleri veya ilişkili oldukları siber saldırı olayı ile ilgili şifreli analiz bilgilerine ve raporlara, platform üzerinden şifrelendirilmiş olarak ulaşabilmekte ve cihazlarında görüntüleyebilmektedir. Siber savunma analistleri, aynı uygulama üzerinden olay çözümlemesinde bulunabilmekte, olayla ilgili verilere erişebilmekte ve vaka raporlarını düzenleyebilmekte, diğer analistlerle şifreli anlık yazışma arayüzü ile iletişim kurabilmektedir.

Buluşun Kısa Açıklaması

Bu buluşun amacı, siber savunma merkezlerinde karşılaşılan vakalara ilişkin otomatik olarak kayıt oluşturulmasını, merkeze yeni vaka geldikçe oluşan kayıtlar üzerinde sorgu yapılarak anlık bilgilendirmeler yapılmasını sağlayan bir sistem gerçekleştirmektir.

Bu buluşun bir başka amacı, yetkili kullanıcılara vakaya ilişkin sorgu sonuçlarının şifrelenmiş biçimde gönderilmesiyle sonuçların yalnızca şifreyi açan yetkili kullanıcılar tarafından görüntülenmesini sağlayan çift katmanlı bir sistem gerçekleştirmektir.

Buluşun Ayrıntılı Açıklaması

Bu buluşun amacına ulaşmak için gerçekleştirilen "Siber Savunma Merkezlerinde Vaka Bildirimi Sağlayan Bir Sistem" ekli şekilde gösterilmiş olup, bu şekil;

Şekil-1; Buluş konusu sistemin şematik bir görünüşüdür.

Şekillerde yer alan parçalar tek tek numaralandırılmış olup, bu numaraların karşılıkları aşağıda verilmiştir.

1. Sistem
2. Vaka veri depolama modülü
3. Elektronik cihaz
4. Vaka sorgulama mobil uygulaması

Buluş konusu siber savunma merkezinin karşılaştığı siber tehditlerin ilgili harici kaynaklara bildirilmesini sağlayan bir sistem (1);

- siber saldırılara ilişkin verileri depolamak üzere yapılandırılan en az bir vaka veri depolama modülü (2),
- üzerinde en az bir uygulama çalıştırmak üzere yapılandırılan en az bir elektronik cihaz (3),
- elektronik cihaz (3) üzerinde çalışmak ve vakaya ilişkin sorguları vaka veri depolama modülüne (2) erişerek cevaplamak üzere yapılandırılan en az bir vaka sorgulama mobil uygulaması (4) içermektedir.

Buluş konusu sistemde (1) yer alan vaka veri depolama modülü (2) vaka müdahale süreçlerine dahil olan tüm vakalara ilişkin verileri depolamak üzere yapılandırılmaktadır. Vaka veri depolama modülü (2) vakalara ilişkin verileri önceden belirlenmiş şifreleme yöntemleri doğrultusunda şifreleyerek depolamak üzere yapılandırılmaktadır.

Buluş konusu sistemde (1) yer alan elektronik cihaz (3) firma çalışanı, firma direktörü gibi siber savunma yetkilisi kullanıcıların kullandığı cep telefonu, tablet, bilgisayar gibi bir cihazdır. Elektronik cihaz (3) üzerinde en az bir uygulama çalıştırmak üzere yapılandırılmaktadır.

Buluş konusu sistemde (1) yer alan vaka sorgulama mobil uygulaması (4) elektronik cihaz (3) üzerinde çalışmak ve yetkili kullanıcının vakaya ilişkin sorgu

yapmasını mümkün kılmak üzere yapılandırılan en az bir arayüz içermek üzere yapılandırılmaktadır. Vaka sorgulama mobil uygulaması (4) vaka veri depolama modülüne (2) erişerek yeni vaka kaydı gerçekleştiğinde yetkili kullanıcıya bildirim göndermek üzere yapılandırılmaktadır. Vaka sorgulama mobil uygulaması (4) yetkili kullanıcının mevcut vakalara ilişkin bilgi istemesini, sorgu yapmasını mümkün kılmak üzere yapılandırılmaktadır. Vaka sorgulama mobil uygulaması (4) vaka veri depolama modülünde (2) şifrelenmiş biçimde depolanan vaka kayıtlarına ilişkin sorgu yapıldığında erişim izni olan yetkili kullanıcılara şifrelenmiş vaka kaydını iletmek üzere yapılandırılmaktadır. Vaka sorgulama mobil uygulaması (4) vaka kaydının okunabilir olmasını sağlayan şifreyi yetkili kullanıcıya iletmek üzere yapılandırılmaktadır. Vaka sorgulama mobil uygulaması (4) şifreyi açan yetkili kullanıcının vaka kaydını görüntülemesini mümkün kılmak üzere yapılandırılmaktadır. Buluşun bir uygulamasında vaka sorgulama mobil uygulaması (4) sorgu sonuçlarını bir rapor biçiminde yetkili kullanıcının önceden tanımlanmış olan e-posta adresine göndermek üzere yapılandırılmaktadır. Bahsedilen uygulamada vaka sorgulama mobil uygulaması (4) yetkili kullanıcıya raporu görüntülenebilir kılan bir şifre göndermek üzere yapılandırılmaktadır.

Buluş konusu sistemde (1) öncelikle bir vaka veri depolama modülüne (2) gerçekleşen tüm vakalara ilişkin kayıtlar açılmaktadır. Bu kayıtlar önceden belirlenmiş bir şifreleme yöntemine uygun biçimde şifrelenmektedir. Vaka depolama modülüne (2) yeni kayıt geldiğinde, yetkili kullanıcıya ait elektronik cihaz (3) üzerinde çalışmakta olan vaka sorgulama mobil uygulaması (4) yetkili kullanıcıya otomatik olarak bildirim göndermektedir. Vaka sorgulama mobil uygulaması (4) yetkili kullanıcının vaka veri depolama modülü (2) üzerinde sorgu yapmasını sağlamaktadır. Yetkili kullanıcının yaptığı sorguya ilişkin şifrelenmiş sorgu sonuçları ve sonuçların şifresi yetkili kullanıcıya elektronik cihaz (3) üzerinde çalışmakta olan vaka sorgulama mobil uygulaması (4) üzerinden iletilmektedir. Şifreyi çözen yetkili kullanıcı, vakaya ilişkin sonuçları vaka sorgulama mobil uygulaması (4) üzerinden anlık olarak görüntüleyebilmektedir.

Bu temel kavramlar etrafında, buluş konusu sistem (1) ile ilgili çok çeşitli uygulamaların geliştirilmesi mümkün olup, buluş burada açıklanan örneklerle sınırlandırılamaz, esas olarak istemlerde belirtildiği gibidir.

Şekil 1