BİLGİ GÜVENLİĞİ YÖNETİMİNDE VARLIKLARIN RİSK DEĞERLENDİRMESİ İÇİN BİR MODEL

Hidayet Takçı, Türker Akyüz, Alper Uğur, Rahim Karabağ, İbrahim Soğukpınar
Gebze Yüksek Teknoloji Enstitüsü
Bilgisayar Mühendisliği Bölümü
{ htakci, takyuz, augur, rkarabag, ispinar}@bilmuh.gyte.edu.tr

ABSTRACT

Risk evaluation and management is an important part of Information Security Management Systems. Therefore lots of risk analysis and evaluation research has been conducted and there are many publications in literature. In this work, a risk evaluation model is proposed for assets related Information Security Management Systems. In our model risk of assets is evaluated using the changing attributes of assets for each threat. Our model has been tested for sample assets of a generic network.

Keywords: Information security, security management, risk analysis, risk assessment, risk management,

1. GİRİŞ

Çağımızda bilgi, kişi ve kurumlar için en önemli varlık haline gelmiştir. Bilginin kurumların yapı ve işleyişindeki önemi nedeniyle, üretilmesi, işlenmesi, iletilmesi ve saklanması sırasında güvenliğinin sağlanması hayati öneme sahiptir. Bu amaçla, kurumlar için bilgi güvenliği yönetim sistemleri (BGYS) için değişik modeller önerilmiştir.[1]

Bilgi güvenliği yönetimi "Bilginin gizliliği, bütünlüğü ve kullanılabilirliği ve onu destekleyen süreç ve sistemlerle ilgili riskleri yönetmek için gerekli denetim ortamının kurulması ve bakımının yapılması " olarak tanımlanmaktadır [2]. Bu amaçla bilgi güvenliği yönetimi için farklı yöntemler geliştirilmiş ve standartlar tanımlanmıştır [3,4]. Tanımlanan standartlarda bilgi güvenliği yönetim sisteminin ilk adımı güvenlik politikasının tanımlanması ve risk yönetimidir. Varlıklara yönelik risklerin belirlenmesi ve bu risklere karşı önlem alınması bilgi güvenliği yönetiminin en önemli adımını teşkil etmektedir.

Varlıklar için risk basit olarak "Oluştuğu zaman varlığın değerini azaltan bir olayın olasılığı" şeklinde tanımlanabilir [5]. Risk hesabında ise, olayın olma (tehdit) olasılığı ile olayın olduğu (tehdidin meydana geldiği) durumdaki değer kaybının çarpımı o varlık için söz konusu olay için risk'in değerini verecektir. Örneğin bir varlık için virüs riski, virüs bulaşma olasılığı ile bulaşan virüsün hasar etkisinin çarpımı olarak hesaplanır.

Bilgi güvenliğinde varlıkların risklerini hesaplamak için nicel ve nitel yöntemler geliştirilmiştir [5, 6, 7]. Bu yöntemlerin geniş analizi Vostare ve Labuschande tarafından yapılmıştır [7]. Ancak konu güncel olduğu, bilgi güvenliğinde etken olan varlıklar için riskler çok ve değişik olduğu için bilgi güvenliğinde risk analizi ve yönetimi konusunda hala yeni araştırmalar yapılmaktadır.

Bu çalışmada, bilgi güvenliği yönetiminde, varlıkların risklerini hesaplamak için, varlıkların özniteliklerine dayalı (kapsamlı) bir yöntem önerilmiştir. Risk hesabında varlık öznitelikleri ve bu özniteliklerin bir tehdidin oluşması durumundaki değişimi esas alınmaktadır. Yöntem örnek bir yapı için sınanmıştır.

2. BİLGİ GÜVENLİĞİ YÖNTEMİ VE VARLIK YÖNETİMİ

İlgili Çalışmalar

Risk değerlendirmesi, risk yönetimi sürecini oluşturan önemli bileşenlerden biridir. Risk değerlendirmesinden alınacak sonuçlar, diğer risk yönetimi faaliyetleri için bir temel oluşturur. Özellikle uygun politikaların seçilmesi ve bu politikaları uygulamak için kullanılacak tekniklerin belirlenmesi konularında esas teşkil eder.

Risk değerlendirmede çoğunlukla kullanılan genel yaklaşım varlık/tehdit/açıklık modeli tabanlıdır. Bu model varlık, tehdit ve açıklıkların belirlenmesi, risklerin bulunması ve uygun etkin kontrollerin seçilip uygulanması esasına dayanır. NIST tarafından hazırlanan bilgi sistemleri için risk yönetimi rehberinde, risk değerlendirmesi süreci şu dokuz adımdan oluşur: 1. Sistem karakterizasyonu, 2. Tehditlerin tanımlanması, 3. Açıklıkların tanımlanması, 4. Kontrol analizi, 5. Tehditlerin gerçekleşme ihtimallerinin tespiti, 6. Etki analizi, 7. riskin hesaplanması, 8. Kontrol önerileri ve 9. Sonuçların dokümantasyonu [8].

Bilgi güvenliğindeki risklerin değerlendirilmesi, diğer tip risk değerlendirmelerine göre oldukça

zordur zira bilgi güvenliği risk faktörlerinin ihtimal ve maliyetleri hakkındaki bilgiler daha sınırlıdır ve sürekli değişmektedir. Örneğin bir saldırganın sisteme zarar verebilecek bir saldırı gerçekleştirme ihtimalini ile ilgili bilgiler sınırlıdır veya saldırı sonucunda hassas bilginin açığa çıkmasından kaynaklanan kaybın maliyetinin sayısal veriye dönüştürülmesi oldukça zordur [9].

Risk değerlendirme amacıyla kullanılan metot ve modeller, yapılacak değerlendirmenin kapsamına ve risk faktörleri ile ilgili verilerin biçimine göre çeşitlilik gösterir. Risk değerlendirme yöntemleri genel olarak nicel ve nitel yaklaşımlar şeklinde ikiye ayrılır. Nicel yaklaşımda riskin ve riski azaltmak için kullanılacak yöntemlerin finansal maliyeti matematiksel ve istatistiksel yöntemler ile hesaplanır. Bu hesap, olayın gerçekleşme ihtimali, potansiyel kayıpların maliyeti ve alınacak karşı önlemlerin maliyeti kullanılarak yapılır. Eğer elimizde gerçekleşme ihtimali ve maliyetler ile ilgili güvenilir bir bilgi mevcut değilse, riskin düşük, orta ve yüksek gibi daha öznel terimlerle ifade edildiği ve uzmanlık gerektiren nitel yaklaşım kullanılabilir.

Nitel yaklaşımın avantajı riskleri derecelerine göre kolayca sıralayabilmesi ve acil iyileştirme gerektiren alanların tanımlanabilmesidir. Ancak nitel yaklaşım, sayısal değerler vermediğinden uygulanacak kontrollerin kâr-maliyet analizini yapmak zordur ve uzmanlık gerektiren öznel bir yaklaşım olduğundan farklı zamanlarda farklı sonuçlar verebilir. Nitel yaklaşım tabanlı risk değerlendirme metotlarına örnek olarak COBRA' yı [10] verebiliriz. COBRA, incelenen organizasyonun yapısına göre kendi yazılımını kullanarak bilgi tabanlı anketler üretir ve organizasyonun çok büyük uzman yardımına ihtiyaç duymadan kendi kendine risk değerlendirmesi yapmasına olanak sağlar.

Öte yandan, nicel risk değerlendirme yaklaşımının en büyük avantajı, uygulanacak kontrollerin kâr-maliyet analizinde kullanılabilecek, olayın gerçekleşmesi halinde oluşacak etkinin değerini ortaya koyabilmesidir. Dezavantajı ise elde edilen sayısal değerin anlamının yeterince açık olmaması ve sonucun nitel bir değere dönüştürülme gerekliliğidir. Nicel yaklaşıma örnek metotlara CRAMM [11] ve ISRAM [6] modellerini sayabiliriz. CRAMM metodu aynı isimli yazılım tarafından desteklenen ve ISO 17799 standardına uyumlu nicel bir risk analiz yöntemidir. ISRAM modelinde ise genel risk formülü temel alınmıştır. Bu formül şu şekildedir:

Risk = Güvenlik ihlalinin olma olasılığı x ihlalin yapacağı etki

ISRAM yöntemi yedi temel adımdan oluşur. İlk adımda bilgi güvenliği probleminin tespiti yapılır. İkinci adımda tehditlerin gerçekleşme olasılıklarını etkileyen faktörler sıralanır ve her bir faktörün ağırlığı belirlenir. Sonraki adımda bu faktörler anket soruları ve cevapları şekline getirilir, altıncı adımda risk hesaplanırken bu sorulara verilen cevaplardan elde edilen sayısal değerler kullanılır. Dördüncü adımda anketlerden elde edilen bilgilerin sayısal bilgilere dönüştürülmesinde kullanılacak olan risk tabloları hazırlanır. Beşinci adımda, anketler ilgili kişilere uygulanır. Son adımda ise elde edilen sonuçlar değerlendirilir.

3. RİSK DEĞERLENDİRME MODELİ

Bu çalışmada önce riskin faktörlerinden varlık değerinin nasıl hesap edileceği incelenmiş ve daha sonra riske sebep örnek bir tehdit ele alınarak risk hesabının nasıl yapılacağı gösterilmiştir.

Varlık değerini bulmadan önce tümden gelim yaklaşımı ile önce varlıkların bilgi güvenliği ile ne derece ilgili olduklarına bakacak ve varlık kategorilerini tip bilgisi yardımıyla işaretleyeceğiz. Ardından herhangi bir varlık için risk değerlendirmesi yaparken tip bilgisinden faydalanılacaktır.

Bilgi varlığı ve ilişkili varlıkları 4 kategori veya tip halinde incelemek gerekirse karşımıza şunlar çıkacaktır;

a. (Tip1) Bilgi varlıkları
b. (Tip2) Bilgiyi tutan (depolayan)varlıklar – depolama üniteleri, sunucular v.s.
c. (Tip3) Bilgiyi taşıyan varlıklar – ağ elemanları
d. (Tip4) Bilgiyi işleyen varlıklar – insan beyni ve makine işlemcisi

P(Tehdit) : Tehdidin meydana gelme olasılığı ve
|Varlık| : Varlık değeri olmak üzere;

$$Risk = P(Tehdit) \times |Varlık| \quad (1)$$

Şeklinde elde edilebilir.

Risk hesaplama denklemine göre tehdit olasılığı ve varlık değerinin bulunması bir ihtiyaçtır. Tehdit olasılıkları için yaklaşık değerler araştırmalar sonrasında elde edildiği için bu çalışmada varlık değerinin nasıl elde edilebileceği üzerinde durulacaktır. Varlık değerini hesap etmede varlığın özniteliklerinden faydalanmanın iyi bir yöntem olacağı düşünülerek öncelikle varlık öznitelikleri ve bu öznitelikler ile varlık kategorileri arasındaki ilişkiler Tablo 1'de ortaya konmuştur.

Bu çalışmada varlık değeri olarak varlığın olası kayıp değeri (varlığın özniteliklerinde meydana gelecek değişim miktarı) kullanılacaktır. Böyle bir

tercihin sebebi, özniteliklerdeki olumsuz yönde meydana gelen her değişimin riski biraz daha artırmasıdır.

Sıra	Öz.ID	T1	T2	T3	T4	Açıklama
1	FIYAT	-	X	X	X	Varlığın ederi
2	TAMIRAT	-	X	X	X	Tamirat bedeli
3	OMUR	-	X	X	X	Ekonomik Ömür
4	SAHIP	X	X	X	X	Sahiplik
5	HUKUK	X	-	-	-	Hukuki
6	A.BILESEN	-	X	X	X	Üst bileşene bağlı mı?
7	U.BILESEN	-	X	X	X	Alt bileşeni var mı?
8	SUREC			X		Sürecin bir parçası mı?
9	KULLANICI	-	X	X	X	Kullanıcı durumu
10	AKTIF	-	X	-	-	Aktif kullanım durumu
11	SORUMLU	X	X	X	X	Sorumlusu var mı?
12	HASSAS	X	X	X	X	Hassas bir varlık mı?
13	OGRENME	-	-	-	X	Öğrenebilen, bir varlık mı?
14	KAMU	-	X	X	X	Kamu malı mı?
15	SIGORTA	-	X	X	-	Sigorta durumu
16	YENILENME	X	X	X	X	Yenilenme durumu
17	YAS	-	X	X	X	Kaç yıldır kullanımda
18	GARANTI	-	X	X	-	Garanti durumu
19	BILGI	X	X	X	X	Bilgi değeri
20	ARIZA	-	X	X	-	Arıza durumu

Tablo 1. Bütün varlıklar için olası açıklayıcı öznitelikler

Varlık öznitelik değerlerini ifade etmede 5 seviyeli bir yapı kullanılmış ve her bir öznitelik değeri "Çok Düşük, Düşük, Orta, Yüksek ve Çok Yüksek" değerlerinden birini almıştır. Özniteliklerdeki değişimleri sayısal olarak ifade etme ihtiyacı dolayısıyla bu seviyeler sayılarla eşleştirilmiş ve;

Çok düşük=0, Düşük=1, Orta=2, Yüksek=3 ve Çok yüksek=4

Değerleri atanmıştır.

Varlık özniteliklerinden biri olan ARIZA özniteliği için örnekleme yapmak gerekirse; öncelikle ARIZA özniteliği varlık kategorilerinden donanımsal varlıklar kategorisine girmektedir. Bir donanımda hiç arıza olmaması durumu Çok Düşük (0) ile sunulabilir. Eğer çok az sayıda arıza meydana gelmişse bu donanım için öznitelik değeri Düşük (1) olacak, eğer ara sıra hata veriyorsa Orta (2) değeri verilecek, eğer bu donanım sıklıkla hata veren bir donanım ise buna verilecek değer Yüksek (3) olacaktır. Donanım kullanılamayacak hale gelmişse bunun değeri Çok Yüksek (4) olur.

Her tehdit varlıklar için farklı derecede değer kayıplarına sebep olabilir. Tehdidin şiddetine göre varlık öznitelik değerlerindeki değişim farklı olacaktır. Modelimiz için en hafif etki 1 birimlik bir değişime sebep olurken en ağır etki 4 birimlik bir değişime sebep olacaktır.

Tehdit, tehdide maruz kalan varlık ve tehdit sonucu meydana gelen değer kayıplarına göre risk değerinin hesap edildiği algoritma aşağıdaki gibi olacaktır.

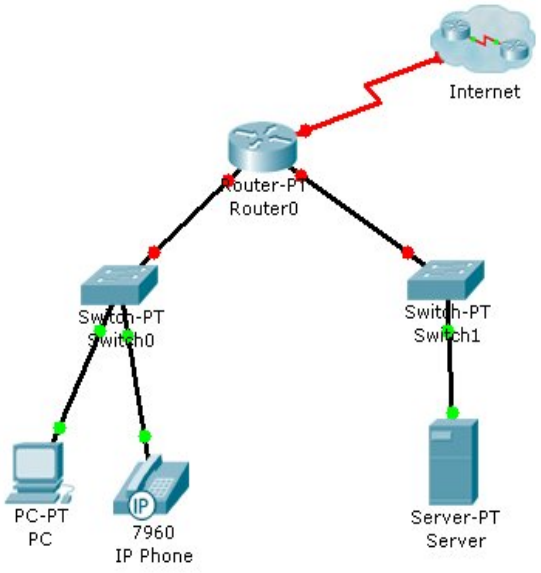
1. Bir tehdit ele al (T_i) i=1,2,…n
2. Tehdidin olasılığını set et ($P(T_i)$ değeri)
3. Bu tehdide maruz kalabilecek varlıkları işaretle ($V_i=(v_{1i},v_{2i},\ldots,v_{mi})$) , j=1,2,…m
4. Tehdide maruz kalan varlıkların sonuna kadar bu işlemleri tekrarla
   a. Tehdide maruz kalan varlıklardan bir tanesi seç
      i. Tehdit bu varlığın hangi özniteliklerini etkilemektedir, işaretle ($Oz_{ji} = Oz_{1ji}, Oz_{2ji} \ldots Oz_{zji}$), k=1,2,…,z
      ii. İşaretlenen öznitelikler için sırayla ne kadarlık değer kaybına sebep olduğunu bul ($\Delta(Oz_{kji})$)
      iii. Değer kayıplarını topla ve bunu tehdidin sebep olduğu değer kaybı olarak sakla ($Toplam_{ji} = \sum_k \Delta(Oz_{kji})$)
      iv. Tehdit olasılığı değeri ile toplamı çarp ($Risk_{ji} = P(T_i) * Toplam_{ji}$)
      v. Elde edilen değer geçerli tehdit ve geçerli varlık için Risk değerini verecektir.
   b. Elde edilen risk değerini risk değerleri tablosuna yazdır.

Şekil 1. Risk değerlendirme algoritması

4. UYGULAMA SONUÇLARI VE ANALİZ

Bir önceki bölümde ayrıntıları verilen modeli örnek bir mimari ve örnek bir tehdit için uygulayarak riskin nasıl hesap edileceği bu bölümde gösterilecektir.

Şekil 2'de verilen örnek ağ modeli için risk değerlendirilmesi bu kısımda yapılmıştır.



Şekil 2. Risk değerlendirmesi yapılan örnek ağ.

Tablo 2'de yanlış yapılandırma tehdidinden etkilenmesi olası varlıklar ile etkilenmeleri halinde hangi varlık özniteliklerinde ne miktar bir değişim meydana geleceği ve önerdiğimiz yönteme göre risk değerlerinin ne olacağı sunulmuştur.

Şekil 2 üzerinde sol alt köşede yer alan cihaz riski bulunacak cihaz olsun. Öncelikle deneye konu olan cihaz kişisel kullanıma yönelik bir bilgisayardır. Bu bilgisayar için yanlış yapılandırma tehdidi olasılığı P(T)=0.88'dir. Bu tehdit tarafından etkilenen varlık öznitelikleri 4, 8, 10 ve 12'dir. Yani, yanlış yapılandırma tehdidi ile SAHIPLIK, SUREC, AKTIFLIK ve HASSASIYET özniteliklerinde değer kaybı meydana gelmektedir. Bunların her biri için değer kayıpları sırayla; 2, 3, 3 ve 2'dir ve toplam değer kaybı ∑Δoz=2+3+3+2=10'dur. Tehdidin olma ihtimali de 0.88 idi, böylece Risk= 0.88 x 10 = 8.8 değerini buluruz.

Bulunan bu değeri yorumlamak için iki seçenek vardır. Bunlardan birisi ağdaki bütün varlıklar için risk değerleri bularak bunları birbiri ile karşılaştırmak suretiyle en büyük risk taşıyanı bulmak diğeri ise elde edilen sayısal değerlerini bir aralık değeri ile karşılaştırmak ve böylece riskin seviyesini ortaya koymak.

Ağ üzerindeki varlık	**YANLIŞ YAPILANDIRMA**					
	P(t)	V	Oz	Δoz	∑	Risk
1. Konaklar						
1.1 Sunucular						
1.1.1 web sunucuları	0.3	X	4,8,10,12	,2,3,3,2	10	3
1.1.2 e-posta sunucuları	0.3	X	4,8,10,12	2,3,3,2	10	3
1.1.3 dosya/ftp sunucuları	0.5	X	4,8,10,12	2,3,3,2	10	5
1.1.4 DNS	0.19	X	4,8,10,12	2,3,3,2	10	1.9
1.2 Bilgisayarlar						
1.2.1 genel kullanım	0.6	X	4,8,10,12	2,3,3,2	10	6
1.2.2 kişisel kullanım	0.88	X	4,8,10,12	2,3,3,2	10	8.8
1.2.3 göreve özel	0.46	X	4,8,10,12	2,3,3,2	10	4.6
1.3 Ağ yazıcısı						
1.4 IP Phone	0.3	X	4,8,10,12	2,3,3,2	10	3
2. Ağ Cihazları						
2.1 hub	0					
2.2 modem	0.3	X	4,8,10,12	2,3,3,2	10	3
2.3 switch	0.19	X	4,8,10,12	2,3,3,2	10	1.9
2.4 router	0.26	X	4,8,10,12	2,3,3,2	10	2.6
2.5 kablosuz router	0.44	X	4,8,10,12	2,3,3,2	10	4.4
2.6 firewall	0.4	X	4,8,10,12	2,3,3,2	10	4
3. İletişim kanalı						
3.1 Bakır kablolu iletişim	0					
3.2 Fiber iletişim	0					
3.3 Kablosuz iletişim	0					

Tablo 2. Yapılandırma tehdidi için örnek risk değerlendirme Tablosu

Birinci duruma göre ağdaki bütün varlıklar için risk değeri hesaplandığında riski en yüksek olanın 8.8 değeriyle kişisel kullanım bilgisayarı olduğu dolayısıyla ağdaki en fazla risk taşıyan (yüksek risk) elemanın o olduğu ortaya çıkar.

İkinci duruma göre ise min-max normalleştirmesi yapılabilir. Min-max normalleştirmesinde her bir risk değeri için yeni değerler bulunur. Bulunan yeni değerler 0-1 Aralığında olacak olup bu değerler için aralıklar duruma göre verilebilir. Normalleştirilen risk değeri $risk^1$ olsun.

$$Risk^1=(risk-min\_risk)/(mak\_risk-min\_risk)$$

Elde edilen risk değerlerini yorumlamada Tablo 3'teki gibi aralıklar belirlenerek varlıkların risk gruplarını bulunabilir;

Risk Aralığı	Risk Değeri
0-0,2	Düşük
0,21-0,50	Orta
0,50-1	Yüksek

Tablo 3. Risk aralıkları

Tablo 2'de elde edilen değerler bu düzene göre yeniden risk gruplarına atıldığında Tablo 4 deki risk değerleri elde edilir.

Varlık	Risk	Risk[1]	Nitel
1.1.1 web sunucuları	3	0,16	Düşük
1.1.2 e-posta sunucuları	3	0,16	Düşük
1.1.3 dosya/ftp sunucuları	5	0,45	Orta
1.1.4 DNS	1.9	0	Düşük
1.2.1 genel kullanım	6	0,59	Yüksek
1.2.2 kişisel kullanım	8.8	1	Yüksek
1.2.3 göreve özel	4.6	0,39	Orta
1.4 IP Phone	3	0,16	Düşük
2.2 modem	3	0,16	Düşük
2.3 switch	1.9	0	Düşük
2.4 router	2.6	0,101	Düşük
2.5 kablosuz router	4.4	0,36	Orta
2.6 firewall	4	0,304	Orta

Tablo 4. Nitel risk değerleri

Tablo 4 ile elde edilen değerler nicel olarak değer üreten modelimizin nitel değerlere dönüşümünü ifade etmektedir. Esasen nicel yaklaşımla çalışan modelimiz nitel verilere de çevrilerek anlaşılırlığı artırılabilir.

5. SONUÇ VE ÖNERİLER

Bilişim sistemlerinde sıklıkla yer alan açıklıklardan kaynaklanan tehditlerin bilişim sistemlerine farklı seviyelerde zararı dokunacak ve bunlar değer kaybı olarak karşımıza çıkacaktır. Her bir tehdidin varlığa ne oranda değer kaybettirdiği bilgisi ile tehditlere göre riskler bulunabilir ve değer kayıplarının hesabından riski hesap etmek mümkün hale gelir.
Bu çalışmada nicel değerler ile risk hesabı yapan bir model önerilmiş ve bir senaryo üzerinden model gerçeklenmiştir. Sonuçlar iki farklı yöntemle yorumlanmış ve benzer çalışmalar için örnek ortaya konmuştur.

KAYNAKLAR

1. JHP. Eloff, MM. Eloff: 2005. Information security architecture. Computer Fraud and Security, 11 / Nov, 2005, pp 10-16.
2. Rolf Moulton, Robert S. Coles, Applying Information Security Governence", Computers&Security, Vol 22 No 7, , 2003 pp 580-584.
3. ISO/IEC 17799, Information Technology-Code of practice for Information security management. Switzerland: Internetional Organization for standardization (ISO); 2000.
4. ISO/IEC 27001, Information Security Management Systems – requirements, ISO 2005
5. Bob Blakley, Ellen McDermott, Dan Geer: "Information security is information risk management" NSPW 2001: 97-104
6. B.Karabacak , İ.Soğukpınar, "ISRAM: Information Security Risk Analysis Method", Computers&Security, Volume 24, Issue 2, Pages 147-159, March 2005
7. A. Vorster and L. Labuschagne. A framework for comparing different information security risk analysis methodologies. In Proceedings of *SAICSIT '05:* pages 95-103
8. National Institute of Standards and Technology (NIST). Risk management guide for information technology systems 2001. Special Publication 800-30
9. United States General Accounting Office (USGAO). Information security risk assessment, <http://www.gao.gov/cgi-bin/getrpt?GAO/AIMD-00-33>; 1999.
10. C&A Systems Security Limited. COBRA consultant products for windows. Evaluation & user guide; 2000.
11. United Kingdom Central Computer and Telecommunicaiton Agency (CCTA). Risk analysis and management method, CRAMM user guide, Issue 2.0; 2001.
12. Howard, 1997 Howard JD. An analysis of security incidents on the internet 1989–1995. PhD thesis, Carnegie Mellon University; 1997.