İSTANBUL TEKNİK ÜNİVERSİTESİ ★ ENERJİ ENSTİTÜSÜ

NÜKLEER TESİSLERDE BİLİŞİM EMNİYETİ

YÜKSEK LİSANS TEZİ

Gökhan AKAR

Enerji Bilim ve Teknoloji Anabilim Dalı

Enerji Bilim ve Teknoloji Programı

ARALIK 2015

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ ENERJİ ENSTİTÜSÜ

NÜKLEER TESİSLERDE BİLİŞİM EMNİYETİ

YÜKSEK LİSANS TEZİ

Gökhan AKAR
301991068

Enerji Bilim ve Teknoloji Anabilim Dalı

Enerji Bilim ve Teknoloji Programı

Tez Danışmanı: Prof. Dr. İskender Atilla REYHANCAN

ARALIK 2015

İTÜ Enerji Enstitüsü'nün 301991068 numaralı Yüksek Lisans Öğrencisi Gökhan AKAR, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "NÜKLEER TESİSLERDE BİLİŞİM EMNİYETİ" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. İskender Atilla REYHANCAN** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Prof. Dr. Üner ÇOLAK** İstanbul Teknik Üniversitesi	.....
	Doç. Dr. Ayşe DURUSOY Yıldız Teknik Üniversitesi	.....

Teslim Tarihi : 26 Kasım 2015

Savunma Tarihi : 28 Aralık 2015

Eşime, anneme ve babama ithafen,

ÖNSÖZ

Enerjinin ne kadar önemli olduğunu artık savaşlar bize gerçek bir şekilde öğretti. Enerji kaynağı sahibi olmak bazen güç sahibi olmaya, bazen de sizi elde etmek isteyenler ile mücadeleye götürüyor.

Bu kaynakların en ilgi çekeni ve belki de en güçlüsü nükleer enerjidir. Gerek enerji üretimi, gerekse savunma sanayiindeki etkisi ile ülkelerin ekonomik ve askeri olarak güçlülüklerinin de ifadesi olmuştur.

Fosil yakıtlardan petrol konusunda henüz zengin olmayan ülkemiz için nükleer enerjiden yararlanmanın er ya da geç başlayacağını düşünüyoruz. Bu bağlamda bilim adamları olan bizlerin de o günler için birşeyler üretmesi ve milli olarak üretilebileceklerimizin azamisini sağlamak, dışarıya olan bağımlılığın azalması bizi daha güçlü kılacaktır.

Çalışan bir nükleer tesisin hizmet vermesini engellemek veya onu bir bomba haline getirmek için artık eskisi gibi fiziksel olarak içeriye sızmak veya dışarıdan fiziksel bomba atma gibi araçlara olan ihtiyaç azalmıştır, çünki artık bilişimin gücü herşeyi ve her yeri etkilemektedir.

TAEK'in tanımlamasına göre nükleer emniyet; nükleer maddelerin barışçıl amaçlar dışında kullanımının önlenmesi ve birey, toplum ve çevrenin radyasyonun zararlı etkilerinden korunması için söz konusu maddelerin ve bunları ihtiva eden tesislerin her türlü hırsızlığa/sabotaja karşı korunmasına yönelik alınan tedbir ve faaliyetlerin tümüdür [1]. Nükleer güvenlik ise, nükleer tesislere ilişkin tüm faaliyetler sırasında, birey, toplum ve çevrenin radyasyonun olası zararlı etkilerinden korunması [2] olarak tanımlanmıştır. Bilişim emniyeti (IT Security) konusundaki ISO 27000 ve ISO 15048 nolu standartların Türkçe ön sayfalarında "IT Security" için "Bilgi Güvenliği" çevirisi kullanılıyor ve konumuz her ne kadar bilişim ağırlıklı olsa da, nükleer tesisler özelinde olduğu için, yerel otorite olan TAEK'in tanımlamasını kullanacağız ve "Bilişim Emniyeti" diyeceğiz.

Bu çalışmamız, nükleer tesis konusunda henüz daha erken safhalarda olan ülkemizin yapılmakta olan ve yapılacak nükleer tesislerinin bilişim saldırılarından korunması bağlamında katkı gayesi ile yazılmıştır.

Bu tezi hazırlamamda bana ufuk açan ve her aşamada hem moral hem de kaynak olarak destekleyen kıymetli hocam Prof. Dr. İskender Atilla REYHANCAN' a ve yine tecrübesinden yararlandığım Zeyneb CAMTAKAN hanımefendiye teşekkürlerimi borç bilirim.

Kasım 2015

Gökhan AKAR
Elektronik ve Haberleşme Müh.

İÇİNDEKİLER

Sayfa

KISALTMALAR

BEP : Bilişim emniyeti planı
BES : Bilişim emniyet sorumlusu
BT : Bilgi Teknolojileri
DoS : Hizmet Engelleme Saldırısı (Denial of Service)
EKS : Endüstriyel Kontrol Sistemi (Industrial Control System)
IAEA : International Atomic Energy Agency (Uluslararası Atom Enerjisi Ajansı)
I&C : Instrumentation & Control (Enstrümantasyon ve kontrol)
ISO : International Organization for Standardization (Uluslararası Standardizasyon Örgütü)
IT : Information Technologies (Bilgi Teknolojileri)
NRC : Nuclear Regulatory Commision (Amerika Birleşik Devletleri Nükleer Mevzuat Komisyonu)
PLC : Programmable Logic Controller (Programlanabilir Mantıksal Denetleyici)
SCADA : Denetim, kontrol ve veri toplama sistemi (Supervisory Control And Data Acquisition)
TAEK : Türkiye Atom Enerjisi Kurumu
TET : Tasarıma Esas Tehdit
VPN : Sanal özel ağ (Virtual Private Network)

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

NÜKLEER TESİSLERDE BİLİŞİM EMNİYETİ

ÖZET

Bu çalışmada nükleer tesislerin bilişim emniyeti konusunda takip edilmesi ve dikkat edilmesi gereken hususlar konusu çalışılmış, doğrudan çözüm bulmak yerine metodoloji önerilmiştir.

Önerilen metodoloji tesisin bütün paydaşlarını göz önüne almakta ve genel bir politika ve farkındalığın varlığına katkıda bulunmaktadır. Bilişim emniyetinin göz ardı edilmesi veya yeterince önemsenmemesi durumunda, dünyadaki meydana gelen olaylardan bahsedilmiş, ayrıca olabilecek senaryolarla örneklendirilmiştir.

Nükleer tesisler hem bilgi teknolojileri hem de endüstriyel kontrol sistemleri şebekelerini içerirler. Her birinin ayrı olarak incelenmesi gerekir. Tesis için endüstriyel kontrol sistemleri daha önemlidir, emniyeti daha hassas şekilde ele alınmalıdır.

Öncelikle tehditlerin neler olabileceği tespit edilmelidir. Bilişim emniyeti hayat döngüsünde bu tehditlerin hangi aşamalarda nasıl oluşabileceği belirlenmelidir. Saldırgan profilleri çıkarılmalı ve bunlara karşı farklı önlemler düşünülmelidir.

Organizasyonel durumlar da ele alınmalıdır. Kurum yönetimi, tesis için bilişim emniyetinin öneminin farkında olmalıdır. Bilişim emniyeti sorumlusu seçimindeki kriterleri özenle belirlemelidir. Kurumun bir **Bilişim Emniyeti Politikası** olmalıdır. Bu politika uygulatılabilir, başarılabilir, denetlenebilir olmalıdır. Bu politika kültür haline gelmeli ve herkes kendi sorumluluğunun farkında olmalıdır.

Politika, plan halinde uygulanmalıdır. Plan içinde organizasyon ve sorumluluklar, varlık yönetimi, risk, zaaf ve uyumluluk değerlendirmesi, sistem emniyet tasarımı ve konfigürasyon yönetimi, operasyonel emniyet prosedürleri ve personel eğitimi konuları işlenmelidir. Eğitim programları düzenlenmeli, bilişim emniyeti farkındalığı, sürekli gelişme yöntemleri veya tekrar eğitim ölçümleri konularını da içermelidir. Bu planın diğer emniyet alanları ile etkileşimi de düşünülmelidir.

Bilişim sistemleri emniyetine kademeli bir yaklaşım olmalıdır. Böylelikle bir saldırının potansiyel sonuçları için orantılı emniyet önlemleri uygulanır. Kademeli yaklaşımın bir pratik kurulumu; bilişim sistemini alanlara bölmek ve o alana has seviyede kademeli önleyici tedbirleri uygulamaktır.

2011 yılında yapılan tahminlere göre insan hatası kökenli emniyet ihlallerin oranı %60-80 arasındadır. Bu oran bize insan hataları üzerinde de ciddi tedbirler almamız gerektiğini göstermektedir. Bilişim emniyeti açısından ve sistem devamlılığı için çalışanların, genel bilişim emniyeti planındaki rollerinin önemini güçlü bir şekilde anlamaları, kendi sorumlulukları tarafındaki gerekli bilişim emniyeti bilgisi ve becerisi, etkin bir emniyet kültürünün kendileri ile başladığının anlaşılması çok önemlidir.

Olası saldırılar için önceden senaryo çalışmaları yapmak faydalı olacaktır. Bu konuda yararlanılabilecek bir çizelge oluşturulmuş ve bundan örnek senaryolar üretilmiştir.

Sonuç olarak bütüncül bir yaklaşım önerilmiş, bir nükleer tesiste olası tüm saldırılabilecek varlıklar açısından genel bir bakış ile nükleer tesislere özel tam bir koruma yönteminin metodolojisi yakalanmaya ve önerilmeye çalışılmıştır.

COMPUTER SECURITY AT NUCLEAR FACILITIES

SUMMARY

In this thesis, the Computer Security at Nuclear Facilities has been studied, instead of giving certain advice details, the approaching methodology has been given.

Nuclear facilities must abide by requirements set by their national regulatory bodies which may directly or indirectly regulate computer systems or set guidance. Nuclear facilities may have to protect against additional threats which are not commonly considered in other industries. Such threats may also be induced by the sensitive nature of the nuclear industry. Computer security requirements in nuclear facilities may differ from requirements in other concerns. Typical business operations involve only a limited range of requirements. Nuclear facilities need to take a wider base or an entirely different set of considerations into account.

The following logical process, described also in detail in IAEA Nuclear Security Series No. 17 publication Section 5, highlights how a nuclear facility can develop, implement, maintain and improve computer security:

—Follow regulatory requirements;

—Examine relevant IAEA and other international guidance;

—Ensure senior management support and adequate resources;

—Define a computer security perimeter;

—Identify the interactions between computer security and facility operation,

nuclear safety and other aspects of site security;

—Create a computer security policy;

—Perform risk assessment;

—Select, design and implement protective computer security measures;

—Integrate computer security within the facility's management system;

—Especially be aware that Industrial Control Systems are vital;

—Keep auditing, reviewing and improving the system.

One of The Facility Management's responsibilities should be to ensure proper coordination of the various disciplines of security and integration of computer security at the appropriate level.

Management should be aware that computer technology is being increasingly used for many vital functions at nuclear facilities. This development has brought multiple benefits to operational safety and efficiency. Nonetheless, to ensure the correct functionality of a computer system, they are required to have adequate and balanced

security barriers to maximize protection against malicious acts without unnecessarily hampering system operations.

Management systems must be reviewed to ensure completeness and compliance with site security policies. More generally, management systems are by nature dynamic and must adapt to changing conditions in the facility and in the environment; they cannot be implemented as a one-off measure but need continuous assessment and improvement.

Protection requirements should reflect the concept of multiple layers and methods of protection (structural, technical, personnel and organizational) that have to be overcome or circumvented by adversaries in order to achieve their objectives.

The primary means of preventing and mitigating the consequences of security breaches is ‘defence in depth’. Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail or be defeated before a computer system compromise could occur. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to computer system compromise, and that the combinations of failures that could give rise to a computer incident are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of defence in depth.

Organizational issues should be considered too. A facility’s senior management should initiate computer security by establishing an adequate process and support organization. Computer security touches almost all facility activities. It is therefore important to assign overarching computer security oversight to one well defined body. It is essential for the Computer Security Officer to have access to adequate interdisciplinary expertise associated with computer security, facility safety, and plant operations as well as physical and personnel security. This may consist of a dedicated computer security team or ad hoc access to specific expertise within the organization.

Each person within an organization is responsible for carrying out the computer security plan. By this methodology, each stakeholder has been considered to be aware of computer security issues. Developing a security culture, building a computer security policy, continuous improvement of program should be planned.

A computer security policy sets the high level computer security goals of an organization. The policy must meet appropriate regulatory requirements. Computer security policy requirements should be factored into lower level documents, which will be used to implement and control policy. Additionally, the policy must be:

—Enforceable;

—Achievable;

—Auditable.

The computer security plan is the implementation of that policy in the form of organizational roles, responsibilities, and procedures. The plan specifies and details the means for achieving the computer security goals at the facility and is a part of the overall Site Security Plan.

The security of computer systems should be based on a graded approach, where security measures are applied proportional to the potential consequences of an attack. One practical implementation of the graded approach is to categorize computer systems into zones, where graded protective principles are applied for each zone based on the level of security requirement assigned to the zone. The assignment of computer systems to different levels and zones should be based on their relevance to safety and security.

Zone borders require decoupling mechanisms for data flow in order to prevent unauthorized access and also to prevent errors from propagating from a zone with lower protection requirements to a zone with higher ones. Technical and administrative measures ensuring the decoupling of zones have to be geared to the individual demands of protective levels. A direct connecting passage through several zones should not be allowed.

Risk assessment is also an important tool for determining the best location to allocate resources and effort in addressing vulnerabilities and the likelihood of their exploitation.

We have also mentioned some IT and Industrial Control Systems security based Nuclear Facility attacks, some more scenarios that might happen. Nuclear facilities contain both Information Technologies Systems and Industrial Control Systems. Both are important but Industrial Control Systems are more important for nuclear facilities and its security should be considered more detailed.

Primarily the threats and attacker profiles should be identified. In creating attack scenarios, one may differentiate between several possibilities. The nuclear facility may be attacked with the purpose of:

—Building up a later coordinated attack intended to sabotage the plant and/or

to remove nuclear material;

—Endangering human or environmental safety;

—Launching an attack towards another site;

—Creating confusion and fear;

—Gaining monetary profit for a criminal group of people;

—Creating major market instabilities and gains for selected market players.

Depending on the objectives or aims of the attack, the attacker will try to

exploit different system vulnerabilities. Such attacks can lead to:

—Unauthorized access to information (loss of confidentiality);

—Interception and change of information, software, hardware, etc. (loss of integrity);

—Blockage of data transmission lines and/or shutdown of systems (loss of availability);

—Unauthorized intrusion into data communication systems or computers (loss of reliability).

All these aspects can have major consequences and impacts on the functionality of computer systems, which may, directly or indirectly, compromise the safety and security of the facility.

The computer security at Nuclear Facilities should be considered in depth from each perspective which we have noticed. Briefly we can emphasize that each stakeholder should be aware of importance of computer security, it should be a culture, and be kept by regulations.

1. GİRİŞ

1.1 Nükleer Tesislerde Bilişim Emniyetinin Önemi

Bilişim emniyeti özellikle son on yılda, ortaya çıkan olaylar ile ne kadar önem verilmesi gerektiğini ortaya koymuştur. Wikileaks'in devletlerin gizli belgelerini sızdırması ve halka açık yayınlaması bunun en bilinir örneği olmuştur.

Emniyet önemine haiz bilgilerin korunması ve sadece onaylanmış kişilerin erişmesi konusu devlet bazında elbette her konu için önemlidir. Fakat bu tezin konusu olarak nükleer tesisler için gerekli olan veri erişim ve saklama emniyet konuları incelenecektir.

Nükleer tesislerin gerek hayati olan enerji temini konusundaki görevi, gerekse yanlış bir durum veya kazada çevreye olan radyoaktif zararları göz önüne alınırsa, siber-teröristler veya olası düşman güçler için oldukça göz önündeki hedefler olduğu aşikârdır.

Siber emniyet bağlamında alınacak tedbirler bağlamında ISO/IEC 27000 standardı çıkmıştır. IAEA, ISO 27000'in temel işlevselliği ve faydalılığını göz önünde bulundurarak, nükleer tesisler özelindeki durumlara yönelik olarak Aralık 2011'de IAEA Nuclear Security Series No.17 adında bir doküman yayınladı [3]. Bu tezin temelini bu çalışma oluşturmaktadır.

1.2 Geçmişte Yaşanmış Bazı Nükleer Tesis Siber Saldırıları Ve/Veya Etkilenmeleri

1.2.1 Stuxnet solucanı ile İran uranyum zenginleştirme programına saldırı

17 Haziran 2010 tarihinde bir antivirüs firması, İran'daki bir müşterisinden cihazının durmadan kendiliğinden kapanıp açıldığını bildiren bir e-posta aldı.[4] İran'ın Uranyum zenginleştirme programını tehdit eden bir saldırı olmuştu. İsrail ve ABD tarafından gerçekleştirildiği sanılan saldırı ile Natanz'daki tesislerindeki sistemler

Stuxnet adlı solucandan zarar gördü. Microsoft Windows aracılığı ile yayılan bu solucanın hedefi, mevcut ambargo ile İran'a satılmaması gereken Siemens Endüstriyel Kontrol Sistemleri idi. [5]

Endüstriyel Kontrol Sistemleri (EKS), SCADA sistemleri, programlanabilir mantıksal denetleyiciler gibi diğer küçük kontrol sistem yapılandırmalarında kullanılan kontrol sisteminin genel adıdır. Burada sözü gelmişken, tezimizin amacının dışına çıkmadan, genel olarak endüstriyel kontrol sistemlerinin bileşenlerinden olan SCADA ve PLC'den bahsetmek gerekirse;

- SCADA (Supervisory Control And Data Acquisition): Sahadan veri toplama ve sahadaki aktüatörleri (kontaktör, vana, sinyal lambası vb. son noktadaki sistem elemanları) denetlemek amacıyla kullanılan ve özünde "Alarm tabanlı görüntüleme ve denetleme" bulunduran sistemdir.
- PLC (Programmable Logic Controller) Programlanabilir Mantık Denetleyici olarak dilimize çevrilen PLC'ler, saha seviyesinde bulunan sensörlerden, diğer cihazlardan ve dâhili birimlerinden aldığı verileri önceden yüklenen mantık programı kapsamında değerlendirerek aktüatörleri kontrol eder. [6]

Dolayısıyle PLC'lerin, EKS'nin kontrolü yapan temel kısmı demek doğru bir yaklaşım olur. Bu nedenle hedef olarak PLC'lerin seçilmesi, saldırgan yaklaşımlarını incelediğimizde, genel bir yaklaşım olduğunu tespit etmekteyiz.

Stuxnet, EKS'lere yapılan ilk saldırı değildir, ama PLC'lere kadar inen ilk solucan olmuştur. Stuxnet'in 5 farklı varyantının, 5 farklı İran tesisine saldırdığı bildirilmiştir [7]. ABD kaynaklı bir düşünme kuruluşu olan Institute for Science and International Security tarafından yapılan iddiaya göre İran'daki tesislerde yaklaşık 1000 santrifüj, bu saldırıdan zarar görmüştür [8].

1.2.2 David-Besse solucan enfeksiyonu

25 Ocak 2003 tarihinde Slammer solucanı Microsoft SQL Sunucularının bir zaafını kullanarak etkisini göstermeye başladı ve yaklaşık 10 dakika içinde bu programı taşıyan sunucuların %90'ı etkilendi. Sabit diski etkilemiyor, dosya silmiyordu, etkisi sadece ön bellekte olup, yayılıp etkileyecek başka veritabanı sunucuları bulmaktı. Zararlı bir kodu bulunmamasına rağmen, ağ bağlantılarında yüksek trafiğine sebep oldu ve belli bir süre Bank of America'nın 13.000 ATM makinası çalışamadı,

Continental Airlines'ın birçok uçuşunun iptali yaşandı ve Güney Kore yarım gün interneti kullanamadı [9].

Slammer solucanından etkilenenler arasında Oak Harbor, Ohio'daki David-Besse nükleer güç tesisi de vardı [10]. Solucan buraya, kendilerinin bağlı olduğu grup şirketin bir danışmanının bilgisayarından bulaşmıştı. Solucan tesisin ana ağını ve kontrol sistemleri ağını etkiledi ve personel 4 saat 50 dakika boyunca, reaktör çekirdeğindeki soğutucu sistemleri, sıcaklık algılayıcılar ve radyasyon dedektörlerinden gelen hassas verileri gösteren Güvenlik Parametreleri Görüntüleme Sistemlerine ağdan erişemediler. Bu sistemin 8 saatten uzun bir süre çalışmaması durumunda ABD Nükleer Düzenleme Kurulu'na (NRC – Nuclear Regulatory Commission) bildirilmesi gerekir. Virüs analog cihazları etkilemediğinden, teknisyenler analog ölçüm cihazları üzerinden takip etmek zorunda kaldılar.

David-Besse tesisinin ağ emniyet duvarı vardı ama sorun dışarıdan değil, içeriden olan birisinden kaynaklanmıştı. Bu nedenle kontrol sistemine erişim yolunda, solucan herhangi bir engele takılmadı.

Bu olaydan 5 yıl sonra NRC, nükleer tesislere uzaktan erişimi yasakladı.

Bu solucandan zarar görmemenin kolay bir önlemi vardı: Microsoft tarafından yaklaşık 6 ay evvel yayınlanan bir yamayı yüklemek!

1.2.3 Browns Ferry'nin kapatılması

Amerika Birleşik Devletleri Alabama'daki Browns Ferry nükleer güç tesisinin 19 Ağustos 2006'da 3 nolu ünitesinin kapatılması, sadece bilgisayarların değil, reaktörün kritik parçalarının da siber saldırıdan etkileneceğini göstermiştir. Reaktör devri daim pompalarının ve yoğuşma demineralizerinin çalışmaması, reaktör çekirdeğinin erimemesi için, 3 nolu ünite manuel olarak kapatılması zorunluluğuna sebep olmuştur.

Yoğuşma demineralizeri bir tür PLC'dir, devri daim pompası da ayarlanabilir frekansta motor hızına dayanır. Her ikisi de içlerindeki Ethernet üzerinden haberleşebilen gömülü mikroişlemciler üzerinden haberleşiyorlardı. Tesisin kontrol sistemi ağı, kaldırabileceğinden daha fazla Ethernet trafiği üretti ve bu parçalar çalışmaz oldular.

Browns Ferry'deki durum bir saldırı değildi. Ama saldırının nereden gelirse gelsin, tesisi kapattırabileceğini göstermesi açısından anlamlıdır.

1.3 Nükleer Tesislerin Emniyeti

Nükleer emniyet kavramı; kriminal, kasıtlı veya yetkisiz kişilerce yapılan; nükleer materyal, diğer radyoaktif materyaller, ilgili tesisler veya ilgili işleri hedef alan ve insanlara, tesislere veya çevreye, doğrudan veya dolaylı olarak zararlı sonuçlar doğurabilecek kasti eylemleri engelleme, algılama ve karşılık vermeyi kapsar.

Bu bağlamda Bilişim Emniyeti, bu sonuçları elde etmek için, günden güne artan hayati bir öneme sahiptir. Bu nedenle bu tez içeriğinde, nükleer emniyetin, bilişim ile ilgili olan taraflarına değinilecektir.

Bilgisayar sistemlerini ve ona bağlı nükleer sistemlerine yönelik kötü niyetli eylemler aşağıdaki gibi gruplandırılabilir:

- Sonradan eyleme dönüştürülecek kötü niyetli kasıtların planlama ve icrası için bilgi toplamak
- Tesisin emniyeti veya güvenliği için önemli bir veya daha çok bilgisayarı ve/veya bilişim sistemini devre dışı bırakma veya niteliklerini kısıtlama
- Bir veya daha çok bilgisayarı devre dışı bırakma veya niteliklerini kısıtlayarak başka tarz bir saldırının yolunu açma, fiziksel olarak içeri sızma gibi.

Bilişim emniyetinin hedefleri, genel itibariyle elektronik veri, bilgisayar sistemlerinin veya işlemlerinin gizlilik, bütünsellik ve erişilebilirliği niteliklerinin korunması olarak tanımlanır. Nükleer tesislerin emniyet ve güvenlik işlevlerinde olumsuz etkisi olacak bu veri veya sistemlerdeki bu hedefleri tanımlayarak ve koruyarak, emniyet hedefleri karşılanmış olacaktır.

1.3.1 Nükleer tesislere özel koşullar

Bilişim emniyeti konusunda Nükleer tesislere özel bazı durumlar vardır. Bu nedenle aşağıda bahsedeceğimiz konular mutlaka düşünülmelidir:

- Nükleer tesisler de genel yönetmeliklerde belirtilen Bilişim konularına doğrudan veya dolaylı olarak uymak durumundadırlar. (Örneğin Triga Mark-II reaktörü İTÜ Ayazağa kampüsü içindedir ve bilgisayar Sistemi Enerji Enstitüsü ve İTÜ Bilişim Daire Başkanlığına bağlı personelin belirlediği genel kaidelere uymak durumundadır.)
- Nükleer tesislerin, başka sanayi kollarında görülmeyen kendine has ilave tehditleri göz önüne alması gerekebilir. Mesela bu konu nükleer üretimdeki bazı hassas konuları içerebilir.
- Nükleer tesislerin bilişim emniyet gereksinimleri, diğer endüstri kollarından farklı olabilir.

Tüm bu durumlar düşünüldüğünde aşağıdaki gibi bir mantıksal süreç ortaya çıkmaktadır:

- Kanunlar ve yönetmeliklere uygun olmalıdır
- IAEA ve diğer yetkin uluslararası kurumların önerileri incelenmelidir
- Uzman yönetim desteği ve uygun kaynaklar sağlanmalıdır
- Bilişim emniyetinin sınırları çizilmelidir
- Tesis operasyon, nükleer emniyet ve diğer alanların güvenlik konuları ile bilişim sistemlerinin iletişimi tanımlanmalıdır
- Genel ve yerel bilişim emniyet politikası oluşturulmalıdır.
- Risk değerlendirme analizi yapılmalıdır
- Bilişim emniyet önlemleri, seçilmeli, tasarlanmalı ve kurulmalıdır
- Tesis Yönetim Sistemi ile Bilgisayar Emniyet Sistemi entegre olmalıdır
- Düzenli olarak sistem denetlenmeli, yeniden gözden geçirilmeli ve geliştirilmelidir.

Bilgisayar sistemleri derken donanımsal yapıyı, Bilişim sistemleri derken yazılımsal yapı ve donanımsal yapıyı, verileri ve sistemlerdeki veri girdisi ve çıktısı olan PLC‘lere kadar bütün elemanları kastetmekteyiz. Siber Emniyet, internet ortamı için olan emniyet, Bilişim Emniyeti genel ve tüm alt bileşenleri kapsayıcı kavram olarak kullanılmıştır. Artık tüm sistemlerin ağ şeklinde topolojisinin olması ve internetin

benzer yapıları ve sunucularının (intranet gibi) dahili ağlarda da kullanılmaya başlanması, zaman içerisinde Siber Emniyetin, Bilişim Emniyeti tabiri yerine ikame edileceği kanaatindeyiz.

2. YÖNETİM REHBERİ

2.1 Düzenleyici ve Yönetimsel Öneriler

Devletin görevlerinden biri nükleer tesislerin emniyetini sağlamak olduğu gibi, genel olarak bilişim emniyeti konusunda yasal çerçeveleri çizme konusunda da sorumluluğu vardır. Çünkü bu yapıldığında ve uygun biçimde uygulandığında, nükleer tesislerin güvenliği ve emniyeti konusunda ciddi bir etkisi olmaktadır. Devlet, en azından yasa ve yönetmelikler ile hassas bilgilerin korunması ve tesis ihlallerini ilk adımda engelleyecek gerekli çerçeveyi sağlamalıdır. Bilişim emniyeti ve kurulumu için yasalar, olabilecek başkalarının yanında aşağıdaki konuları da içermelidir:

- Bilişim sistemine olacak saldırılar hakkında kanun
- Terörizm üzerine kanun
- Bilginin açıklanması konusunda kanun
- Kişisel bilgiler ve gizlilik üzerine kanun

Bu kanunların sadece yapılması değil, aynı zamanda devamlı olarak yeni ve gelişen tehditlere karşı gözden geçirilmesi de zaruridir. Ayrıca unutulmamalıdır ki, bilişim sistemlerinin doğasından dolayı, kötü niyetli eylemlerin sadece bu kanunların geçerli olduğu yurt içinden değil, aynı zamanda yurtdışından da gelmesi mümkündür.

2.2 Mevzuat ile İlgili Hususlar

Düzenleyici kurum, işletmecilerin doğru yorumlama ve kurması için gerekli araç ve ortamı sağlayacak yönetmelik yönlendirmesini dikkate almalıdır. Bu konuda ISO standartları ve IAEA yayınlarından faydalanabilir.

Düzenleyiciler, bilişim emniyeti konusunu ele alırken, nükleer madde hırsızlığı ve radyolojik sızıntıya sebep olacak sabotajları göz önüne almalıdır. Bu nedenle genel bilişim emniyeti kanun ve yönetmelikleri düzenlenirken, nükleer tesislere olacak etkileri de düşünülmelidir.

Gerekli önlemler konusundaki çalışmada tüm paydaşlar görüşlerini ifade etmelidir. Düzenleyici kurum, asgari belirleyici standartlarla bile yüksek seviyede bir emniyet sağlayabilmelidir. Daha detaylı önlemler aşağıdaki konuları içerebilir:

- Bilgisayar emniyeti için yönetim taahhüdü
- Bilişim emniyeti konusuna tahsis edilmiş ekip ve yönetici
- Aşağıdaki mevzuları içeren bilişim emniyet kurulum ve uygulama planı:
    - Bilişim emniyetinin sınırlarının belirlendiği
    - Risk tanımı
    - Risk yönetim stratejisi
    - Bilişim emniyeti eğitim ve farkındalık programı
    - İşletim planlarının devamlılığı
- Düzenleyicilerin dâhili ve harici çalışmalarını denetleme ve yeniden gözden geçirme süreci

İlgili düzenlemeler teknik detayları içermemelidir, çünkü bilişimin hızlı doğası gereği, kısa zamanda o teknik geçersiz olabilir. Onun yerine, teknolojiden bağımsız olarak karşılanması gereken sonuçlar belirtilmelidir. Bilişim emniyeti, Saha Emniyet Planı'nın vazgeçilemez bir parçası olarak ilgili kanun veya yönetmelikte yer almalıdır.

2.3 Saha Emniyet Çerçevesi

Saha emniyeti, yönetim sorumluluğunun uhdesi içerisindeki bir konudur ve tüm ilgili düzenlemelere uygunluk konusunun uygulanması, işletilmesi ve proaktif geliştirilmesi konusunu içerir.

Emniyeti içeren tüm konular (personel, fiziksel, enformasyon, bilişim) birbirleri ile etkileşirler ve birbirlerini tamamlarlar. Bir konudaki bir emniyet açığı öteki konularda da açığa sebep olabilir. Bilişim Emniyeti de diğer disiplinler ile kesişen alanlara sahiptir. Bu çalışmadaki öneriler genel Saha Emniyet Çerçevesinin daha geniş çerçevesi bağlamında değerlendirilmelidir. Yönetimin bir görevi de, farklı disiplinler arasındaki koordinasyonunu uygun bir şekilde sağlamaktır.

2.3.1 Bilişim emniyeti politikası

İdarenin öncelikle bilişim teknolojilerinin nükleer tesislerde artık daha çok kullanıldığı konusunda farkındalık sahibi olması gerekmektedir. Bu gelişme, operasyon, emniyet ve verimlilik açısından birçok fayda sağlamıştır. Yine de bilgisayar sisteminin doğru işlevselliğinden emin olmak için sistem operasyonlarını gereksiz yere engellemeden, kötü niyetli eylemlere karşı korumayı artırmak için uygun ve dengeli emniyet engellerine ihtiyacı vardır.

Bu nedenle her nükleer tesisin bilişim emniyet politikası, sahanın en kıdemli emniyet yöneticisi tarafından gözden geçirilmelidir. Bu politika oluşturulurken yasal ve insan kaynaklarına olan etkisi de düşünülmelidir.

2.3.2 Nükleer tesislerdeki bilişim sistemleri

Halen daha birçok nükleer tesis, standart dışı bilgisayar altyapısı, ayarları ve performans durumları içermektedir [1]. Bunlar o tesise veya üreticiye özel endüstriyel kontrol sistemleri, giriş kontrol sistemleri, alarm ve izleme sistemleri ve emniyet güvenlik ve acil durum cevap sistemleri ile ilgili Bilişim Sistemlerini içerebilir. Birçok endüstriyel kontrol sistemi geçici ara protokol kullanmaktadır. Standartlar ile bu ara çözümler arasındaki fark, saha emniyet politikası belirlenirken göz önüne alınmalıdır.

2.3.3 Derinlemesine savunma

Koruma gereksinimleri, saldırı durumunda üstesinden gelmek için gerekli çoklu katman ve koruma metotlarını (yapısal, teknik, personel, organizasyonel) yansıtmalıdır. Derinlemesine savunma, saldırı bilgisayarlara erişmeden, birbirini izleyen ve bağımsız bir dizi koruma seviyelerinin kombinasyonu ile kurulur ve nükleer tesislerin emniyeti için temel bir kavramdır [11]. Eğer engellerden biri aşılırsa hemen ardındaki koruyacaktır. Derinlemesine savunma düzgün kurulduğunda hiçbir teknik, insani veya organizasyonel hata, tek başına bilgisayar sisteminin çökmesine sebep olamayacaktır. Farklı seviyelerdeki öğelerin bağımsız etkisi, derinlemesine savunmanın önemli bir unsurudur.

2.4 Tehdit ortamının değerlendirilmesi

Bilişim emniyeti tehdit ortamı hızla değişen ve gelişen bir senaryodur. Her ne kadar iyi hazırlanmış bir koruma programı mevcut tehditlere karşı dayanıklılığı artırsa da, gelecek zamanda oluşacak tehditlere karşı bir garanti ifade etmez.

Sorumlu devlet otoritesi, periyodik olarak mevcut nükleer tesislerin bilgisayar sistemlerine yönelik saldırı tehditlerini değerlendirmelidir. Devam eden, aktif bir değerlendirmenin olması ve düzenli olarak yönetim ve işletim birimlerinin bilgilendirilmesi hayati önem arz etmektedir.

2.4.1 Tehditlerin karşılanması

Bir tehdidin karşılanması, ille de tehdidin ortadan kaldırılması anlamına gelmez; söz konusu tehdidin yeterli ölçüde azaltılması ya da etkilerinin yeteri kadar hafifletilmesi anlamına da gelebilir.

Bir tehdidin ortadan kaldırılmasına ilişkin örnekler aşağıdadır:

- Tehdit unsuru tarafından kötü niyetli eylemlerin gerçekleştirilmesi yeteneğinin ortadan kaldırılması,
- Kötü niyetli eylemin varlığa artık bir etkisi olamayacak bir biçimde, değerli varlığın değiştirilmesi, yerinin değiştirilmesi veya korunması,
- Tehdit unsurunun ortadan kaldırılması (örneğin, sık olarak ağın çökmesine neden olan bir aygıtın ağdan çıkarılması).

Bir tehdidin azaltılmasına ilişkin örnekler aşağıdadır:

- Bir tehdit unsurunun kötü niyetli eylemler gerçekleştirme yeteneğinin kısıtlanması,
- Bir tehdit unsuruna kötü niyetli bir eylem gerçekleştirme fırsatı verilmesinin kısıtlanması,
- Gerçekleştirilen kötü niyetli bir eylemin başarılı olma şansının azaltılması,
- Caydırma yoluyla bir tehdit unsurunun, kötü niyetli bir eylem gerçekleştirme motivasyonunun azaltılması,
- Tehdit unsurunun daha üst düzeyde bir uzmanlık ve daha fazla kaynak ihtiyacı duymasının sağlanması

Bir tehdidin etkilerinin hafifletilmesine ilişkin örnekler aşağıdadır:

- Varlığın sık sık yedeklemesinin yapılması,
- Bir varlığın fazladan kopyalarının çıkarılması,
- Bir varlığın sigortalanması,
- Uygun karşı tedbirin alınabilmesi maksadıyla başarılı olan kötü niyetli eylemlerin zamanında tespit edilmesinin sağlanması.

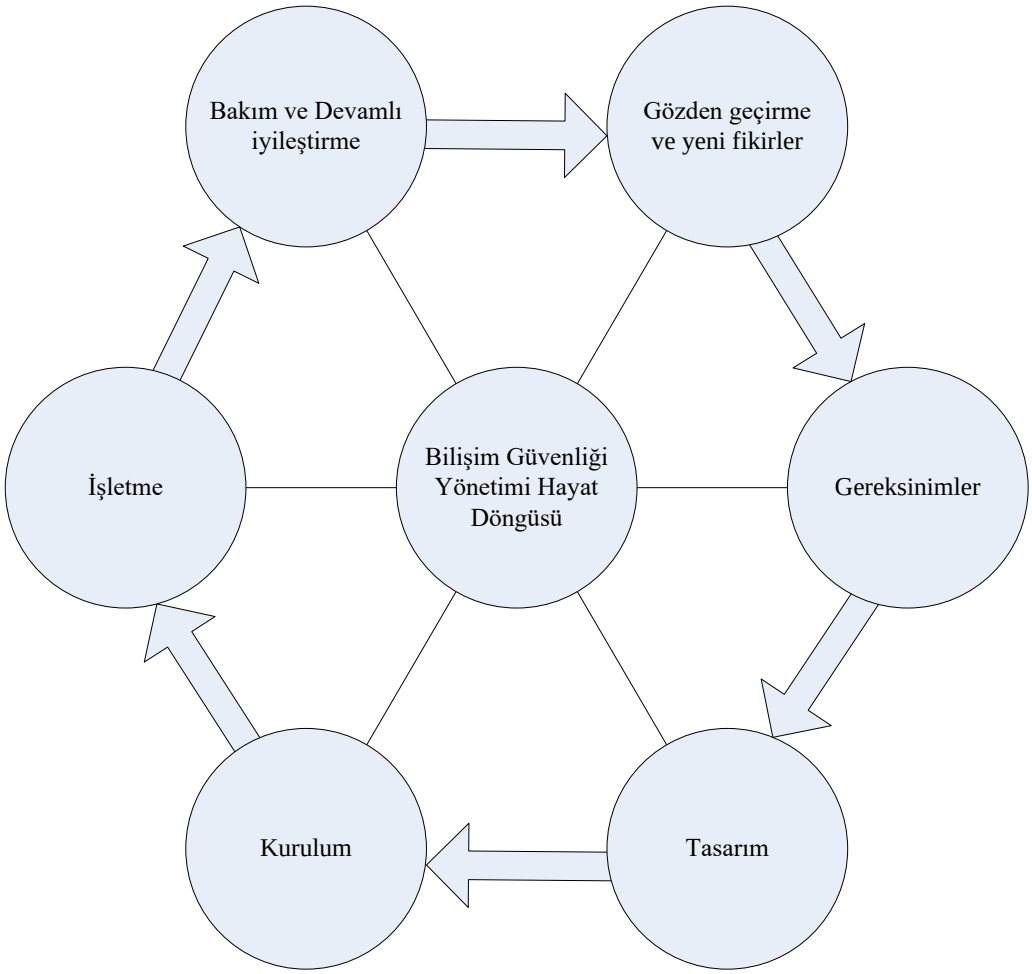
3. YÖNETİM SİSTEMLERİ

Yönetim sistemi, politika ve hedef oluşturma ve hedefleri verimli ve etkin bir şekilde başarmayı sağlamaktan sorumludur. Yönetim sistemleri, nükleer emniyet kültürüne hayati destek elemanlarıdır. Nükleer tesislerdeki çoğu aktivite, yönetim sistemleri tarafından kontrol edilmektedir. Bunlar idealde güvenlik, emniyet, sağlık, çevre, kalite ve ekonomik elemanları tek bir yönetim aracında bulundurur veya birbirini takviye eden araçları içerir.

Yönetim sistemleri, saha emniyet politikaları ile bütünsellik ve uyumluluk açısından gözden geçirilmelidir. Daha genel olarak yönetim sistemleri tabiatları gereği dinamiktir ve tesisteki ve çevredeki değişikliklere adapte olması gerekir; bir kerelik kurulum ile bırakılamaz, devamlı değerlendirme ve geliştirmeye ihtiyacı vardır. Takip eden sayfadaki Şekil-3.1 yönetim proseslerinin hayat döngüsünü tasvir etmektedir.

Bu bölümümüzün amacı, mevcut yönetim sistemlerine, bilişim emniyet yönetimi hususunda gerekli detaylar ile rehberlik etmektir. Gözden geçirilmesi veya eklenmesi gereken önlemler konusunda anahtar konular aşağıdaki gibidir:

- Bilgi varlıklarının tanımlanması ve sınıflandırılması
- Formal risk analizi
- Yasalara ve mevzuata uygunluk
- İşletme gereksinimleri
- Anahtar roldeki kişiler için yetkinlik gereksinimleri
- İş sürekliliği
- Mantıksal erişim yönetimi
- Sistem yaşam döngüsü emniyeti
- Konfigürasyon yönetimi
- Bilişim emniyetini iyileştirme ve onaylama önlemleri



Şekil 3.1 : Bilişim emniyeti yönetimi hayat döngüsü.

- Tanımlanmış bilişim emniyeti önlemlerinin kurulumu
- Kurulmuş bilişim emniyeti önlemlerinin kabulü
- Onaylanmış bilişim emniyeti önlemleri ile uyumluluk
- Bilişim emniyet vakalarında acil analiz ve uygun raporlama
- Uyumluluk üzerine düzenli raporlama
- İç ve dış birimler tarafından kurulmuş emniyet önlemlerinin düzenli olarak gözden geçirilmesi
- Farkındalık eğitimi
- Yeni riskler ve tanımlanmış risklere değişiklikler
- Yasalar ve mevzuatlardaki değişiklikler

- Bilgi emniyeti için orta-vadeli planlar

Yukarıdaki prosesler, sistemin yaşam döngüsünün tüm safhalarında devam eden eylemler olarak görülmelidir.

4. ORGANİZASYONEL KONULAR

4.1 Yetki ve Sorumluluklar

Bu bölüm, başarılı bir şekilde bilişim emniyeti programını kurmak ve korumak konusunda, yönetim ve uzman kadronun minimum sağlayacakları özelliklerden bahsedecektir.

4.1.1 Yönetim

Bir tesisteki üst düzey yönetim, yeterli bir süreç ve destek organizasyonu kurarak, bilişim emniyetinin ilk adımını atmış olur. Bu başarmak için aşağıdakileri yapmalıdır:

- Bilişim emniyetinin tüm yönleri ile genel sorumluluğunu üstlenmek
- Tesisin emniyet hedeflerini belirlemek
- Kanun ve yönetmeliklere uyulmasını sağlamak
- Tesis için risk kabul seviyesini belirlemek
- İşletmedeki bilişim emniyeti sorumluluklarını belirlemek
- Emniyeti sağlayan farklı birimler arasında sağlıklı bir iletişimi kurmak ve varlığından emin olmak
- Uygulanabilir bir bilişim emniyeti politikasını sağlamak
- Geçerli bir bilişim emniyeti programı kurulabilmesi için gerekli uygun kaynakları sağlamak
- Bilişim emniyeti politikası ve süreçlerinin periyodik denetim ve güncellemelerinden emin olmak
- Eğitim ve farkındalık programlarına destek sağlamak

Genelde kalıcı bilişim emniyeti sürecinin kurulumu, işletmedeki uzmanlara delege edilir.

4.1.2 Bilişim emniyet sorumlusu

Bilişim emniyeti, tesisteki neredeyse bütün işlere temas eder. Bu nedenle iyi tanımlanmış birisine, herşeyi kapsayıcı bir bilişim emniyeti bakışının görevlendirilmesi önemlidir. Bu tezimizde "Bilişim Emniyet Sorumlusu" olarak tanımladığımız kişiye, "Bilişim Teknolojileri Emniyet Sorumlusu" , "Haberleşme Emniyet Sorumlusu" gibi adlandırmalar da olabilir. Hangi isimle tanımlanırsa tanımlansın, bu roldeki kişi, sistemler ile koordineli, departmanların yapılandırılmalarından bağımsız, doğrudan üst yönetime erişebilen ve rapor edebilen bir fonksiyona sahip olmalıdır. BES (Bilişim Emniyet Sorumlusu) bilişim emniyeti konusunda derinlemesine bilgi sahibi ve nükleer tesislerdeki diğer emniyet konuları hakkında da iyi bilgi sahibi olmalıdır. Başka özellikleri de; nükleer güvenlik ve proje yönetimi konusunda bilgili, farklı disiplinlerdeki kişileri entegre çalıştırabilme ve iletişim kurabilme olmalıdır.

BES'nin veya denk pozisyondakinin tipik sorumlulukları aşağıdakileri içerir:

- Kurum veya şirket yönetimine bilişim emniyeti konusunda tavsiyelerde bulunmak
- Bilişim emniyet ekibini yönetmek
- Bilişim emniyet eylemlerinin (emniyet politikasının, direktifler, süreçler, metotlar, önlemlerin oluşturulması) gelişimini kontrol ve koordine etmek
- Fiziksel emniyet ve diğer güvenlik ve emniyet disiplinleri ile koordineli olarak emniyet önlemleri ve emniyet vakalarına tepki planlarını yapmak
- Bilişim emniyeti için kritik öneme haiz sistemleri belirlemek ve o sistem sorumlularının, kendi sistemlerinin bilişim emniyeti içindeki önem ve rolü hakkında bilgilendirmek
- Periyodik bilişim emniyeti değerlendirmelerini yönetmek
- Periyodik olarak teftiş, denetleme ve gözden geçirmeleri yönetmek ve üst yönetime durum hakkında rapor sunmak
- Bilişim emniyeti eğitimi ve değerlendirmesini geliştirmek ve uygulamak
- Bilişim emniyetine yönelik acil durum vakalarına yönelik karşı önlemleri, ilgili iç ve dış organizasyonlar ile koordineli olarak geliştirmek ve yönetmek

- Bilişim emniyeti vakalarını araştırmak ve vaka sonrası süreci ve önleyici eylemleri geliştirmek
- Saha emniyetini değerlendirme girişimlerine (toplantı, denetim vb.) katılmak
- Yeni sistemlerin alımı veya geliştirilmesi için ihtiyaç analizlerine katılmak

4.1.3 Bilişim emniyeti ekibi

Bir bilişim emniyet sorumlusu için bilişim emniyeti, tesis güvenliği, saha operasyonları, fiziksel ve personel emniyeti gibi disiplinler arası konularda uzman bilgisine ulaşması önemlidir. Bu da ancak bu işe özel bir ekibin oluşturulması veya organizasyondaki ilgili kişilere özel erişim hakkı olması ile olacaktır. Bu ekibin görevi BES'na sorumluluğunu gerçekleştirebilme konusunda tamamlayıcı açıdan yardım etmek şeklinde olacaktır.

4.1.4 Diğer yönetim sorumlulukları

Bir işletmedeki değişik yönetim seviyeleri, kendi sorumluluk alanındaki uygun düzeydeki bilişim emniyetini sağlamalıdır. Tipik sorumluluklar aşağıdakileri içerir:

- Saha bilişim emniyeti planı kılavuzluğunda çalışma
- Bilişim emniyeti konusunda BES'na ilgili geri bildirimlerde bulunma ve işletme, güvenlik ve emniyet konuları ile arasındaki potansiyel çatışmaları çözmek
- Personel, ekipman veya süreç değişimi gibi bilişim emniyeti yapısında değişim gerektiren konularda BES'nu bilgilendirmek
- Ekibinin kendi konusunda yeterince eğitimli olması ve kendi konularındaki bilişim emniyeti hakkında kısaca bilgilendirilmesini sağlamak
- Yüklenici ve taşeronlardaki çalışanların saha emniyet planına uygun çalışmalarını sağlamak
- Emniyetle ilgili olayları izleme, görüntüleme ve raporlama
- Personelinin emniyet önlemlerine uygun çalışmasını sağlamak ve zorlamak

4.1.5 Kişisel sorumluluklar

İşletmedeki herkes emniyet planına uymakla sorumludur. Bunlardan konumuza özel bazıları aşağıdaki gibidir:

- Temel bilişim emniyeti süreçleri bilgisi
- İşine özel bilişim emniyeti süreçleri bilgisi
- Bilişim emniyeti politika parametreleri içerisinde çalışmak
- Bilişim emniyetinde azalmaya sebep olabilecek herhangi bir değişiklikten yönetimi haberdar etmek
- Bilişim emniyetinde tavize sebep olabilecek herhangi bir olaydan yönetimi haberdar etmek
- Düzenli olarak emniyet konusundaki başlangıç ve yenileme eğitimlerine katılmak

4.2 Bilişim Emniyeti Kültürü

Güçlü bir bilişim emniyeti kültürü, herhangi bir etkin emniyet planının önemli bir parçasıdır. Bilişim emniyeti farkındalığının genel tesis emniyet kültürüne yerleşmiş olması yönetim için önemlidir. Nükleer emniyet kültürünün temel özellikleri; inançlar, tutum ve davranışlar, yönetim sistemleri ve daha etkin nükleer emniyet programına yönlendirecek birlikteliklerdir. Nükleer emniyet kültürünün temeli, nükleer tesisleri ve eylemleri düzenleme, yönetme, işletme ve hatta bu eylemlerden etkilenebilecek kişilerce, ciddi bir tehdidin varlığını ve nükleer emniyetin önemli olduğunu bilme ve onaylamadır. Bilişim emniyeti kültürü, genel emniyet kültürünün bir altkümesidir ve yukarıda saydığımız temel özelliklerin bilişim emniyeti farkındalığına uygulanmasıdır.

Tecrübeler göstermiştir ki; çoğu bilişim emniyeti vakaları insan kaynaklıdır ve herhangi bir bilgisayar sisteminin emniyeti, onun bütün kullanıcılarının davranışlarına bağlıdır. Bilişim emniyeti kültürü, personeli bilgilendirme ve bilişim emniyeti farkındalığını artırma için tasarlanmış birçok eylemler kümesi (posterler, hatırlatmalar, yönetim tartışmaları, eğitim, testler vb.) ile geliştirilir. Bilişim emniyeti kültürü nitelikleri periyodik olarak ölçülmeli, gözden geçirilmeli ve aralıksız

geliştirilmelidir. Aşağıdaki göstergeler bir organizasyondaki bilişim emniyeti kültürü değerlendirmek için kullanılabilir:

- Bilişim emniyeti gereksinimleri iyi biçimde dokümante edilmiş ve personel tarafından iyice anlaşılmış olması
- Organizasyon içindeki ve dışındaki bilgisayar sistemleri işletimi için net ve etkin yöntemler ve protokollerin varlığı
- Personelin bilişim emniyeti programındaki kontrollere bağlı kalmanın önemini anlamış ve farkında olması
- Bilişim sistemlerinin güvenli ve bilişim emniyeti temelindeki kurallara uygun bir şekilde çalışmasının korunuyor olması
- Yönetimin emniyet ile ilgili girişimlere açık ve destekleyici olması

4.2.1 Bilişim emniyeti eğitim programı

Güçlü bir eğitim programı bilişim emniyeti kültürünün köşe taşlarındandır. Personel, yüklenici ve üçüncü taraf satıcıların, emniyet süreçlerini gözlemlemenin ve emniyet kültürünü korumanın önemi konusunda eğitilmeleri çok önemlidir.

Farkındalık programı aşağıdakileri mutlaka içermelidir:

- Bilişim emniyeti eğitimi ve/veya farkındalık programını başarıyla bitirmiş olmak, bilgisayar sistemine erişim için önkoşul olmalıdır. Eğitim, sistem emniyet seviyeleri ve kişinin organizasyondaki rolü ile orantılı olmalıdır.
- Önemli emniyet sorumlulukları olan kişilere (BES, bilişim emniyet ekibi, proje yöneticileri, bilgisayar sistemi yöneticileri gibi) özel olarak ileri seviye eğitimler ve nitelikler sağlanmalıdır.
- Eğitim bütün personel için, yeni çıkan yöntemler ve tehditler hakkında periyodik olarak tekrarlanmalıdır.
- Personel kendi emniyet sorumluluklarını anladıklarını ve kabul ettiklerini yazılı olarak beyan etmelidirler.

Eğitim programı, bilişim emniyeti farkındalığı, eğitimin etkinliği ve sürekli gelişme yöntemleri veya tekrar eğitim ölçümlerini içermelidir.

5. BİLİŞİM EMNİYETİ KURULUMU

Bu tezimizde kabul edilebilir risklerin minimum standartlarını belirleme yapıyoruz demek yanlış olur. Çünki dijital dünyadaki yeni bir gelişme, yeni tehditlerin çıkması, yeni bilişim araçlarının bulunması ve yönetmeliklerdeki değişmeler bu çalışmayı gündem dışına atabilir. Yaklaşımımız, nükleer tesislerdeki bilişim emniyetinin rehberliği ve desteğine dair metodolojik ve kaya gibi sağlam önerilere odaklanmaktır.

Bu tavsiyeler kesin kurallar değildir ve başvuru kaynağı olabilecek şekilde kullanılmalıdır. Arzu edilen derinlemesine savunma ve diğer temel nükleer emniyet hedeflerini elde etmek için uygun ve alternatif önlemler olarak benimsenebilir.

5.1 Bilişim Emniyet Politikası ve Planı

5.1.1 Bilişim emniyeti politikası

2.3.1. nolu bölümde de bahsettiğimiz üzere bir bilişim emniyeti politikası, bir organizasyondaki yüksek seviye bilişim emniyeti hedeflerini belirler. Bu politika, ilgili yasal gereklilikleri karşılaması gerekir. Bilişim emniyeti politikası gereksinimleri, politikayı kurmak ve kontrol etmek üzere alt seviye belgelere kadar ayrıştırılarak indirgenmelidir. Ayrıca politika;

- Uygulatılabilir,
- Başarılabilir,
- Denetilebilir olmalıdır.

5.1.2 Bilişim emniyeti planı (BEP)

Bilişim emniyeti planı (BEP), belirlenen politikanın organizasyonel roller, sorumluluklar ve yöntemler şeklinde kurulumudur. Plan, tesisteki bilişim emniyeti hedeflerini elde edebilmek için gerekli araç ve ortamları tanımlar, detaylandırır ve genel saha emniyet planının bir parçasıdır. Plan, emniyet açıkları, koruyucu

önlemler, sonuç analizi, karşı duyarlılık, nükleer tesisin kabul edilebilir bir siber risk seviyesini kurmak ve korumak için azaltıcı önlemler ile güvenli işletim durumuna dönüşünü kolaylaştırmak için temel ve ilk eylemleri içermelidir.

5.1.3 BEP bileşenleri

Her ayrı plan parçası, kurulu bilişim emniyeti politikası baz alınarak, kendi farklı hedef ve gayesine ulaşmaya çalışır. BEP için tavsiye edilen minimum içerik ve gruplandırma aşağıdaki gibidir.

a) Organizasyon ve sorumluluklar
   - Organizasyon şemaları
   - Sorumlu kişiler ve raporlaması gereken sorumluluklar
   - Periyodik gözden geçirme ve onaylama süreci

b) Varlık yönetimi:
   - Bütün bilgisayar sistemini listelemek
   - Bütün bilgisayar sistemi uygulamalarını listelemek
   - Bilgisayar ağı şeması (bütün dış bağlantıları dâhil şekilde)

c) Risk, zaaf ve uyumluluk değerlendirmesi
   - Emniyet planı gözden geçirme ve yeniden değerlendirme dönemselliği
   - Öz-değerlendirme (Ağa sızma test prosedürleri dâhil)
   - Denetim yöntemleri ve eksiklik izleme ve düzeltme yöntemleri
   - Yasa ve yönetmeliklere uygunluk

d) Sistem emniyet tasarımı ve konfigürasyon yönetimi
   - Temel bilişim mimarisi ve tasarım ilkeleri
   - Farklı emniyet seviyeleri ile ilgili gereklilikler
   - Bilişim emniyeti gerekliliklerini tedarikçiler için belirli bir düzene koyma
   - Bütün hayat döngüsü emniyeti

e) Operasyonel emniyet prosedürleri

- Erişim kontrolü
- Veri emniyeti
- Haberleşme emniyeti
- Platform ve uygulama emniyeti
- Sistem izleme
- Bilişim emniyetinin bakımı
- Vaka idaresi
- İş devamlılığı
- Sistem yedekleme

f) Personel eğitimi

- Emniyet soruşturması
- Eğitim
- Nitelik
- Sonlandırma /Transfer

Yukarıdakiler bir BEP geliştirilmesi için çerçeve sunmaktadır. Herhangi bir işletme için geçerli olan bu konuların nükleer tesisler için olması gereken farklı detayları ileriki konularda ele alınacaktır.

5.2 Diğer Emniyet Alanları ile Etkileşim

Daha önce de belirttiğimiz gibi BEP, emniyetin diğer konularını da içeren Genel Saha Emniyet Planının bir parçasıdır. Tesise özel bilişim emniyet planı fiziksel koruma, güvenlik, işletme ve bilişim uzmanlarının istişaresi ile geliştirilmelidir. BEP düzenli olarak emniyet alanındaki olaylar ve operasyonel tecrübeler ile gözden geçirilmeli ve güncellenmelidir.

5.2.1 Fiziksel emniyet

Fiziksel emniyet planı ile BEP birbirini tamamlamalıdır. Bilişim varlıklarının fiziksel erişim kontrol sistemleri ile iletişimi vardır, bundandır ki fiziksel emniyetin azalması veya kalkmasına sebep olabilir. Saldırı senaryoları hem fiziksel, hem elektronik olarak ikisi birden planlanmış olabilir. Her iki tarafın ekipleri birbirlerini bilgilendirmelidir ve geliştirme ve gözden geçirme sürecinde koordineli çalışmalıdırlar.

5.2.2 Personel emniyeti

Farkındalık ve eğitimin yanında, emniyetin diğer konuları da -genellikle personel emniyeti tarafınca yapılır- kalıcı bilişim emniyeti için önemlidir. Uygun seviyede emniyet araştırması, gizlilik taahhütleri, gerekli iş yetkinliklerini tanımlama ve iş sonlandırma prosedürleri için gerekli önlemler, bilişim emniyeti ve personel emniyet yönetimleri arasında koordineli olarak gerçeklenmelidir. Özellikle anahtar roldeki kişiler için (emniyet elemanları, sistem yöneticileri gibi) işe başlamadan önceki emniyet araştırması daha derinlemesine olmalıdır.

5.3 Varlık Analizi ve Yönetimi

Nükleer tesislerdeki bilgisayar sistemleri, belirgin olmayan bir şekilde aralarında etkileşebilirler. Bundan dolayı emniyet planının bütün varlıkları tanımlaması, tesisin emniyet ve güvenlik işlevleri için kritik öneme haiz olanlar için daha detaylı envanter çalışmasını içermesi önemlidir. Bu envanter veri, bilgisayar sistemleri, ara yüzlerini ve sahiplerini içermelidir.

Aşağıdaki gibi bir metodoloji, yukarıdaki ihtiyaçları karşılayacaktır:

- Varlıkların tam bir listesini çıkarmak için bilgisayar sistemlerinden ilgili bilgiler derlenmelidir.
- Tanımlanan varlıklar arasındaki ara bağlantılar belirtilmelidir.
- Güvenlik fonksiyonları ile belirlenen güvenlik sistemleri, güvenlikle bağlantılı sistemler ve emniyet sistemi arasındaki ilişki tanımlanmalı ve değerlendirilmelidir.

Her bir adımın tamamlanmış olması, bir sonraki adımın ön şartı olmaktadır.

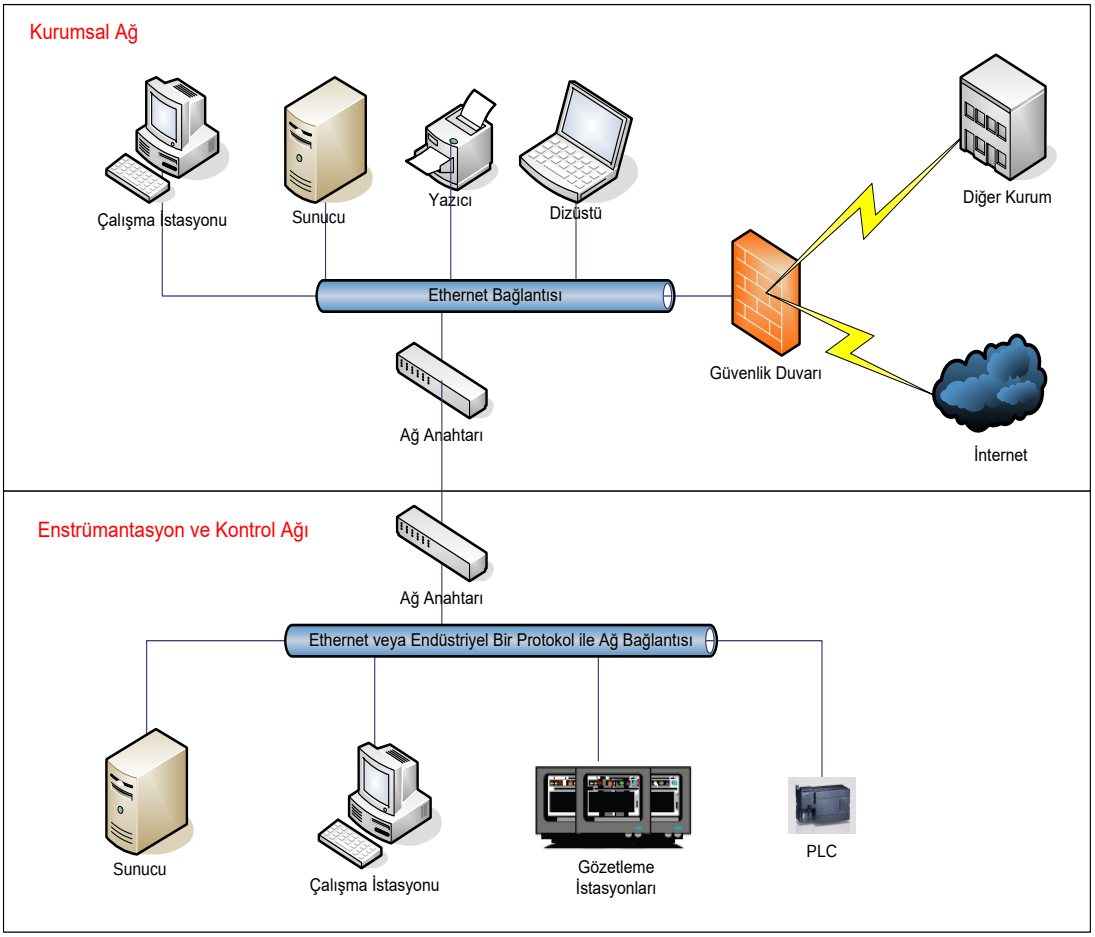
Bir nükleer tesisteki bilgisayar sistemlerinin kapsamlı analizi aşağıdakileri içerir:

- Bütün kompüterize sistemlerin işlevleri/görevleri ve operasyonel durumları
- İlgili ara bağlantıların tanımlanması (güç kaynakları dâhil)
- Ne, ne ile, nasıl ve niçin haberleştiğini anlamak için iş akış analizi
- Haberleşmeyi başlatma prosedürleri, haberleşme sıklığı ve protokolleri
- Bilgisayar sistemleri ve ekipmanlarının yerleşimi
- Kullanıcı gruplarının analizi
- Sahipler (veri ve kompüterize sistemlerin)
- İlgili bilişim emniyeti seviyesi (Bölüm 5.5' deki kademeli yaklaşım)

Analiz için gerekli bilgilerin mevcut olduğu varsayılmıştır. Bununla birlikte harmanlanması ve organize edilmesi gerekecektir. Gerekli bilgiler sistem özellikleri ve dokümantasyonunu içerir. Takip eden sayfada nükleer tesislerdeki bilişim sistemlerinin temsili bir gösterimi Şekil 5.1'de mevcuttur. Bu temsili gösterimde bilişim sistemleri temel anlamda iki ayrı ağ olarak gösterilmiştir. Bunlar "kurumsal ağ" ve "enstrümantasyon ve kontrol ağı" olarak gösterilmiştir.

5.4 Bilgisayar Sistemi Sınıflandırması

Daha önce de belirttiğimiz üzere, bu tezimizin bağlamında bilgisayar, bilgisayar sistemi, bilişim sistemi tabirleri; nükleer tesisteki hesaplama, ölçme, haberleşme ve algılama cihazları gibi işlevsel elemanlardır. Birincil öncelikli ilgilendiğimiz bilgisayar fonksiyonları güvenlik ve emniyetle ilgili kontrol ve veri süreçleridir. Diğer fonksiyonlar ile olan ilgimiz, bu fonksiyonları destekleyici olmaları, ikincil veya dolaylı veya genel tesis üretkenliği ile ilgili emniyet azaltıcı olması durumunda olacaktır.



Şekil 5.1 : Nükleer tesislerdeki bilişim sistemlerinin temsili gösterimi.

5.4.1 Güvenliğin önemi

IAEA, bir nükleer tesisteki ekipmanları fonksiyonlarına göre aşağıdaki gibi sınıflandırmıştır.

<u>Saha Ekipmanları:</u>

- Güvenlik için önemli sistemler
  - Güvenlik sistemleri
    - Koruma sistemleri: Reaktör ve tesis koruma eylemlerinde otomatik olarak başlayan enstrümantasyon[1] ve kontrol sistemleri (I&C)

[1] Enstrümantasyonu geniş anlamda; ölçülebilir fiziksel girdilerin değerlendirilmesi olarak tanımlayabiliriz. Enstrümantasyon proses kontrolü için gerekli verileri sağlar. Proses kontrolü ise basit bir örnekle; tesisin aydınlatma sistemini güneş ışığına bağımlı olarak yönetmek gibi işlemlerdir. Burada güneş ışığının girdisi enstümanlardan alınarak kontrol cihazına girilir ve kontrol cihazı aydınlatmayı kontrol eder.

        - Güvenliği Harekete Geçirme Sistemleri: Koruma sistemleri ve manuel başlatma ile harekete geçen güvenlik eylemlerini yapan I&C sistemleri
        - Güvenlik sistemi destek özellikleri: Acil durum güç kaynağı için I&C
    - Güvenlikle İlişkili Sistemler
        - Süreç kontrol sistemleri: Saha kontrolü için I&C sistemleri
        - Alarm sistemlerini de içeren I&C kontrol odası
        - Kontrol odası için bilgileri toplayan ve hazırlayan Süreç Bilgisayar Sistemleri
        - Yakıt taşıma ve depolama I&C sistemleri
        - Yangın önleme sistemleri
        - Giriş kontrol sistemleri
        - Ses ve veri haberleşme altyapısı
    - Güvenlik için önemsiz sistemler
        - Güvenlik açısında önemsiz işlevler için kontrol sistemleri (demineralizasyon gibi)

Saha ekipmanları açısından önemli olmayıp, bilgisayar sistemi güvenliği açısından önemli olan düşünceler de arz edilmelidir.

<u>Saha dışı ekipmanlar:</u>

- Ofis otomasyonu
    - İş izni ve iş emri sistemleri: Güvenilir bir çalışma ortamını sağlamak için iş eylemleri ile koordinasyonu sağlayan sistemler
    - Mühendislik ve bakım sistemleri: Operasyon, bakım ve teknik destek detaylarını içeren sistemler

- Konfigürasyon yönetim sistemleri: Nükleer tesise kurulan modeller, versiyonlar ve parçaların konfigürasyonlarının saklandığı sistemler
- Belge yönetim sistemleri: Çizimler, görüşme zamanları gibi işletmedeki bilgilerinin saklandığı ve geri çağrıldığı sistemler
- İntranet: Teknik ve idari belgelere erişimi sağlayan sistem Genelde yazma özelliği olmadan yalnız-okuma özellikli dir.

Dış bağlantı:

- E-posta: Dışarıdaki taraflara bilgi aktarımı sağlamak için kullanılan sistem
- Herkese açık internet sitesi: Tesis hakkında internet kullanıcılarına bilgi vermek için kullanılan sistem
- Uzaktan erişim: Sıkı kontrol edilmesi gereken, belirli işlevlerin dışarıdan yapılaması için kurulan sistem

5.4.2 Emniyet sistemleri veya emniyetle ilişkili sistemler

- Fiziksel erişim kontrol sistemleri: Kendi görev ve sorumluluklarına uygun olarak güvenilir kimselerin ilgili bölümlere girmeleri için kullanılan sistem
- Ses ve veri haberleşme altyapısı
- Emniyet erişim veri tabanı: İlgili ve yetkili kişilerin, tesisteki bir yer veya bilgiye erişimlerini saklayan sistem
- Emniyet alarm gözetleme ve kontrol sistemleri
- Bilgisayar ve ağ emniyeti bileşenleri
- Nükleer muhasebe ve kontrol sistemleri

5.5 Bilişim Emniyetine Kademeli Yaklaşım

Bilişim sistemleri emniyetine kademeli bir yaklaşım olmalıdır. Böylelikle bir saldırının potansiyel sonuçları için orantılı emniyet önlemleri uygulanır. Kademeli yaklaşımın bir pratik kurulumu; bilişim sistemini alanlara bölmek ve o alana has seviyede kademeli önleyici tedbirleri uygulamaktır. Farklı seviye ve alanlara ayırma

işlemi bölüm 5.4'te anlatıldığı gibi güvenlik ve emniyetle olan ilişkilerine göre yapılmalıdır. Yine de risk değerlendirme süreci, geri beslemeye ve kademeli yaklaşıma açık olmalıdır.

5.5.1 Emniyet seviyeleri

Emniyet seviyeleri, tesisteki farklı bilişim sistemleri için emniyet koruma derecesinin sınırlarını belirler. Kademeli yaklaşımdaki her seviye, kendi seviyesinin ihtiyaçlarına göre farklı koruyucu önlemler içerir. Bazı emniyet önlemleri bütün seviyeler içindir, bazıları da sadece o seviyeye özeldir.

Emniyet seviyesi modeli, sistemlerin sınıflandırılması temelli olarak farklı bilişim sistemlerine koruyucu önlemlerin uygulanmasını kolaylaştırır.

Seviyeler ve ilgili koruyucu önlemler BEP'nda uygun şekilde dokümante edilmelidir.

5.5.2 Alanlar

Alanlar, koruyucu önlemlerin yönetim, iletişim ve uygulanması için mantıksal ve fiziksel olarak bilişim sistemlerinin gruplanmasıdır. Alan modeli, güvenlik ve emniyet açısından aynı veya benzer bilişim sistemlerinin gruplanmasını sağlar.

Alan modeli uygulanırken aşağıdaki ilkelere uyulmalıdır:

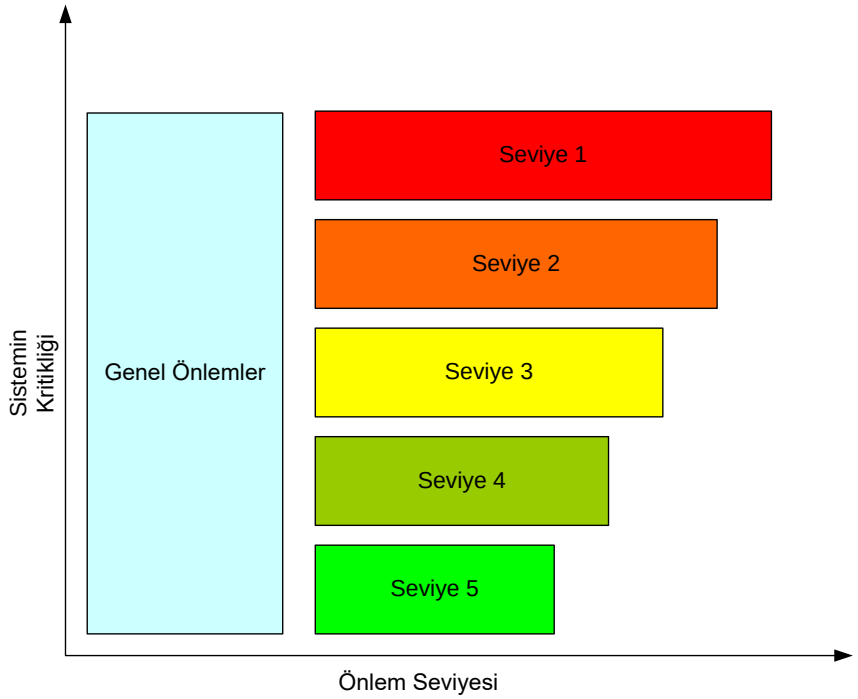
- Her alan, tesisin emniyet ve güvenliği için aynı veya benzer öneme sahip sistemleri içerir.
- Aynı alandaki sistemler, benzer koruyucu önlemlere ihtiyaç duyarlar.
- Aynı alandaki farklı bilişim sistemleri alan içindeki dâhilî haberleşmeleri için güvenilir bir ortam oluştururlar.
- Alan sınırlarında, alan-bağımlı politikalar gereğince oluşturulmuş veri akışını denetleyecek mekanizma olmalıdır.
- Alanlar, konfigürasyonu geliştirmek için alt alanlara bölünebilir.

Alanlar kendi içinde aynı veya benzer bilişim sistemleri içerdiğinden, koruyucu önlemler o alandaki bütün bilişim bileşenlerine uygulanabilir. Bununla birlikte alanlar ve seviyeler arası ilişki birebir değildir; bir seviye, aynı seviye koruma derecesine ihtiyaç duyan birçok alana hitap edebilir. Alanlar mantıksal ve fiziksel gruplandırmadır, seviye ise gerekli koruma derecesini gösterir.

Alan modeli BEP'nda detaylı olarak belirtilmelidir. Bütün bilişim sistemleri, bütün ilgili iletişim hatları, alan kesişmeleri ve harici bağlantıları dokümante edilmelidir.

5.5.3 Bir emniyet seviyesi modeli uygulamasının örneği

Farklı seviyelerdeki emniyet önlemlerinin uygulandığı bir örnek aşağıda anlatılmıştır. Bu sadece kademeli emniyet için sadece bir kurulum örneğidir. Seviyelerin tam seçimi ve onların temel emniyet önlemleri, ilgili ortama, tesis özelliklerine ve ilgili emniyet risk analizine göre ayarlanmalıdır.



Şekil 5.2 : Kademeli emniyet seviyesi uygulaması.

Bu kurulumda:

- Genel önlemler bütün seviyelere ve bütün bilişim bileşenlerine uygulanmalıdır.
- Emniyet seviyeleri Seviye 5'ten (En az emniyet gereken seviye) Seviye 1'e (en çok emniyet gereken seviye) kadar değişmektedir.
- İlgili seviyenin önlemleri kümülatif değildir (Bu nedenle tekrarlar oluşabilir).

5.5.3.1 Genel seviye

Uygulanabilir bütün sistemler ve seviyelerde aşağıdaki genel önlemler uygulanmalıdır.

- Politikalar ve uygulamaları her seviye için tanımlanmıştır.
- Emniyet işletim süreçleri herkes için yazılmıştır ve herkes tarafından okunur.
- Sisteme erişim izni verilen kişiler, uygun niteliklere ve tecrübeye sahiptir.
- Kullanıcılara sadece işlerini yapmaları için gerekli olan sistemlere izin verilmiştir.
- Tesiste uygun bir erişim kontrolü ve kullanıcı denetimi mevcuttur.
- Anomali algılama sistemleri ve prosedürleri mevcuttur.
- Uygulama ve sistem zaafları izlenmektedir ve gerekli önlemler alınmıştır.
- Sistem zaafları değerlendirilmesi periyodik olarak yapılmaktadır.
- Taşınabilir ortamlar (DVD, Flash Bellek, SD kart vb) emniyet işletim prosedürlerine uygun olarak kontrol edilmelidir.
- Bilgisayar ve ağ emniyet bileşenleri iyi bir şekilde korunmalıdır.
- Bilgisayar ve ağ emniyet bileşenleri (emniyet geçitleri (security gateways), ağa sızma algılama sistemleri (intrusion detection systems), ağa sızmayı önleme sistemleri (intrusion prevention systems), sanal özel ağ sunucuları (virtual private network (VPN) servers) loglanmalı ve izlenmelidir.
- Uygun yedekleme ve geriye döndürme prosedürleri mevcuttur.
- İşlevlerine göre bileşenlere ve sistemlere fiziksel erişim sınırlıdır.

5.5.3.2 Seviye 1

Genel önlemlere ek olarak, Seviye 1 koruyucu önlemleri, tesis için hayati olan ve en yüksek seviye emniyet gerektiren “koruyucu sistemler” için kullanılmalıdır. Bu önlemler aşağıdakileri içerebilir:

- Daha zayıf emniyet seviyesindeki hiçbir veri akışının Seviye 1’e girmesine izin verilmez. Sadece dışarıya doğru çıkışı vardır. Bu durumda unutulmamalıdır ki, bu tarz tek yönlü iletişim, haberleşmede güvenilirlik ve

entegre olmayı sağlamaz (yedeklilik ve hata düzeltme konuları ayrıca düşünülmelidir). Ayrıca yine göz ardı edilmemelidir ki, TCP/IP gibi el-sıkışmalı protokollerin de kullanılmaması anlamına gelir. İstisnalara asla iyi gözle bakılmaz ve hatta bazı IAEA ülkelerinde, her ne olursa olsun istisna kabul edilmemektedir.

- Sistemlerin bütüncüllüğü ve erişilebilirliğini sağlayabilmek için olan önlemler güvenlik durumlarının bir parçasıdır.
- Uzaktan bakım-onarıma izin verilmez.
- Fiziksel erişim sıkı kontrol edilir.
- Sistemlere erişim verilen personel sayısı minimumda tutulur.
- Bilgisayar sistemlerinde onaylanmış herhangi bir modifikasyonda iki-kişi kuralı uygulanır. Tek başına hiç kimse karar ve uygulama yapamaz.
- Bütün aktiviteler loglanmalı ve gözlenmelidir.
- Sistemlere her veri girişi, durumdan duruma tabanlı olarak onaylanır ve doğrulanır.
- Donanım bakımı, güncelleme ve yazılım modifikasyonları gibi herhangi bir modifikasyona sıkı organizasyonel ve idari prosedürler uygulanır.

5.5.3.3 Seviye 2

Genel önlemlere ek olarak Seviye 2 koruyucu önlemleri, yüksek seviye emniyet gerektiren operasyonel kontrol sistemleri için olmalıdır. Bu önlemler aşağıdakileri içerebilir:

- Seviye 2'den dışarıya sadece Seviye 3 yönünde tek yönlü veri şebeke trafiğine izin verilir. Sadece, gerekli olduğunda "alındı" mesajları ve kontrol edilmiş işaret mesajları (TCP/IP mesajları) içeri yönde kabul edilir.
- Uzaktan bakım erişimine, vaka bazlı olmak üzere ve tanımlanmış süreli olarak izin verilebilir. Kullanıldığında güçlü önlemler ile korunmalıdır ve kullanıcılar tanımlanmış emniyet politikasına saygı duymalıdırlar (sözleşme gereği)

- Sistemlere erişim izni verilen personelin sayısı minimumda tutulur ve kullanıcı erişim hakları ile yönetici erişim hakları arasında belirgin bir ayrım vardır.
- Sistemlere fiziksel bağlantılar sıkı şekilde kontrol edilmelidir.
- Bütüncüllük ve erişilebilirliği sağlamak adına bütün makul önlemler alınmıştır.
- Sistemlerdeki aksiyonlara yönelik emniyet açığı değerlendirmesi sahayı veya süreci kararsız bir duruma sürükleyebilir, bu nedenle kabul testleri veya uzun süreli kesinti durumlarında, sadece test ortamları ve yedek sistemlerde yapılmalıdır.

5.5.3.4 Seviye 3

Genel önlemlere ek olarak, Seviye 3 koruyucu önlemleri, operasyonlar için kullanılmayan gerçek zamanlı sistemlerin gözetiminde kullanılmalıdır, yani değişik siber tehditler için orta şiddet seviyesindeki, kontrol odasındaki proses gerçek-zamanlı gözetleme sistemleri için. Bu koruyucu önlemler aşağıdakileri içerebilir:

- Seviye 3'ten internete erişime izin verilmez.
- Anahtar roldeki kaynaklar için loglama ve denetim izleri gözetlenir.
- Emniyet geçitleri (Security gateways), 4. seviyeden gelen kontrolsüz trafikten korumak üzere kurulur ve sadece özel ve sınırlı aktiviteye izin verilir.
- Sistemlere fiziksel bağlantılar kontrol edilmelidir.
- Sağlıklı ve güçlü kontrol sağlanması bazında olarak -genel olarak değil- vakadan vakaya uzaktan bakım erişimine izin verilir; uzak bilgisayar ve kullanıcı sözleşmede belirtilen ve tanımlanan emniyet politikasına uymalıdır.
- Kullanıcılara açık sistem fonksiyonları, "bilinmesi gerekli" kaidesi tabanlı olarak, erişim kontrol mekanizmaları tarafından kontrol edilir. Bu kaideye herhangi bir istisna dikkatli çalışılmalı ve koruma başka araçlar (fiziksel erişim gibi) ile sağlanmalıdır.

5.5.3.5 Seviye 4

Genel önlemlere ek olarak, farklı siber tehditler için ortalama şiddet seviyesinde olan ve bakım için kullanılan teknik veri yönetim sistemi veya operasyon için teknik özellikler tarafından gereksinim duyulan sistemler veya parçalarla ilgili operasyon eylem yönetimi tarafından kullanılmalıdır. Seviye 4 önlemleri aşağıdakileri içerir.

- Sistemlere modifikasyonları, sadece onaylanmış ve nitelikli kullanıcılar yapabilir.
- Seviye 4'ten internet erişimi, gerekli koruma önlemleri uygulanmış kullanıcılara verilebilir.
- Emniyet geçitleri (Security gateways) bu seviyede, dışarıdaki şirket veya site ağlarının kontrolsüz trafiğinden korunmak ve kontrol edilmiş özel eylemleri korumak için kurulur.
- Sisteme fiziksel bağlantılar kontrol edilmelidir.
- Uzaktan bakıma izin verilir ve kontrol edilir, uzak bilgisayar ve kullanıcı ise sözleşmede belirtilen ve tanımlanan emniyet politikasına uymalıdır.
- Kullanıcılara açık sistem fonksiyonları, erişim kontrol mekanizmalarınca kontrol edilir. Bu kurala olabilecek herhangi bir istisna, dikkatle çalışılarak kontrol edilmelidir ve başka araçlar/ortamlar aracılığıyla korunma sağlanmalıdır.
- Uygun erişim kontrol mekanizmalarının olduğu yerlerde, dışarıdan kullanıcı erişimi, onaylanmış kişiler için açıktır.

5.5.3.6 Seviye 5

Seviye 5 önlemleri, teknik kontrol veya operasyonel amaçlar için doğrudan önemi olmayan "ofis otomasyon sistemleri" gibi değişik siber tehditler için düşük etki seviye olan yerlerde kullanılmalıdır. Seviye 5 önlemleri aşağıdakileri içerir:

- Sistemlere değişiklikleri sadece onaylanmış ve nitelikli personelin yapmasına izin verilir.
- Seviye 5'ten internet erişimi uygun koruyucu önlemler uygulanarak sağlanır.

- Gerekli kontrollerin olduğu durumlarda, yetkili kişilerin uzaktan haricen erişimlerine izin verilir.

5.5.4 Bölgelerin ayırımı

Bölge sınırlarında, daha az koruma gereken bir bölgeden daha yüksek olana hataların yayılmasını engellemek ve yetkisiz erişimleri engellemek için veri akışı mekanizmaları ayrımına ihtiyaç vardır.

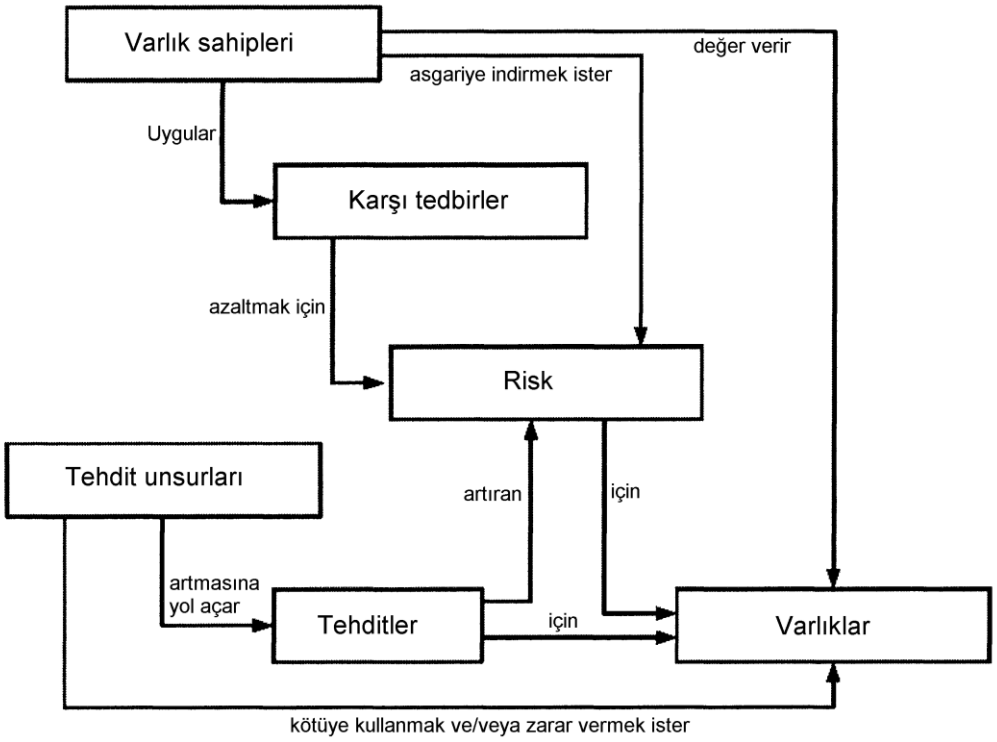
Bölgelerin ayrımını sağlayan teknik ve idari önlemler, her koruyucu seviyenin taleplerine göre ayarlanmalıdır. Birkaç bölgeyi doğrudan geçen bir pasaja asla izin verilmemelidir.

6. TEHDİTLER, ZAAFLAR VE RİSK YÖNETİMİ

Bu bölümde risk yönetiminde kullanılan temel kavramları içermektedir. Risk yönetimi tesisin tasarım, geliştirme, işletim, bakım gibi hayat döngüsündeki her aşaması ile alakalıdır.

6.1 Temel Kavramlar ve İlişkiler

Bilişim emniyeti bağlamında risk, bir varlığın veya bir grup varlığın zayıflıklarından yararlanan ve böylelikle organizasyona zarar verebilecek tehdidin potansiyeli anlamındadır. Bir olayın olma ihtimali ve sonucunun sebep olacağı zarar şiddeti ile ölçülür.



Şekil 6.1 : Emniyet kavramları ve ilişkileri. [12]

6.2 Risk Değerlendirme ve Yönetimi

Risk değerlendirme; kaynakları en iyi şekilde yerleştirme, zaafların belirlenmesi ve suiistimali konusunda önemli bir araçtır.

Tehdit, zaaf ve etkinin özel kombinasyonlarının tanımlanıp dokümante edildiği ve uygun koruyucu kontrollerin tasarlandığı bir süreçtir. Tehdit ve zaaf değerlendirme, bilişim sistemlerine olacak saldırıların sonuçlarını önlemek veya azaltmak için gerekli tedbirler için bir temel teşkil eder.

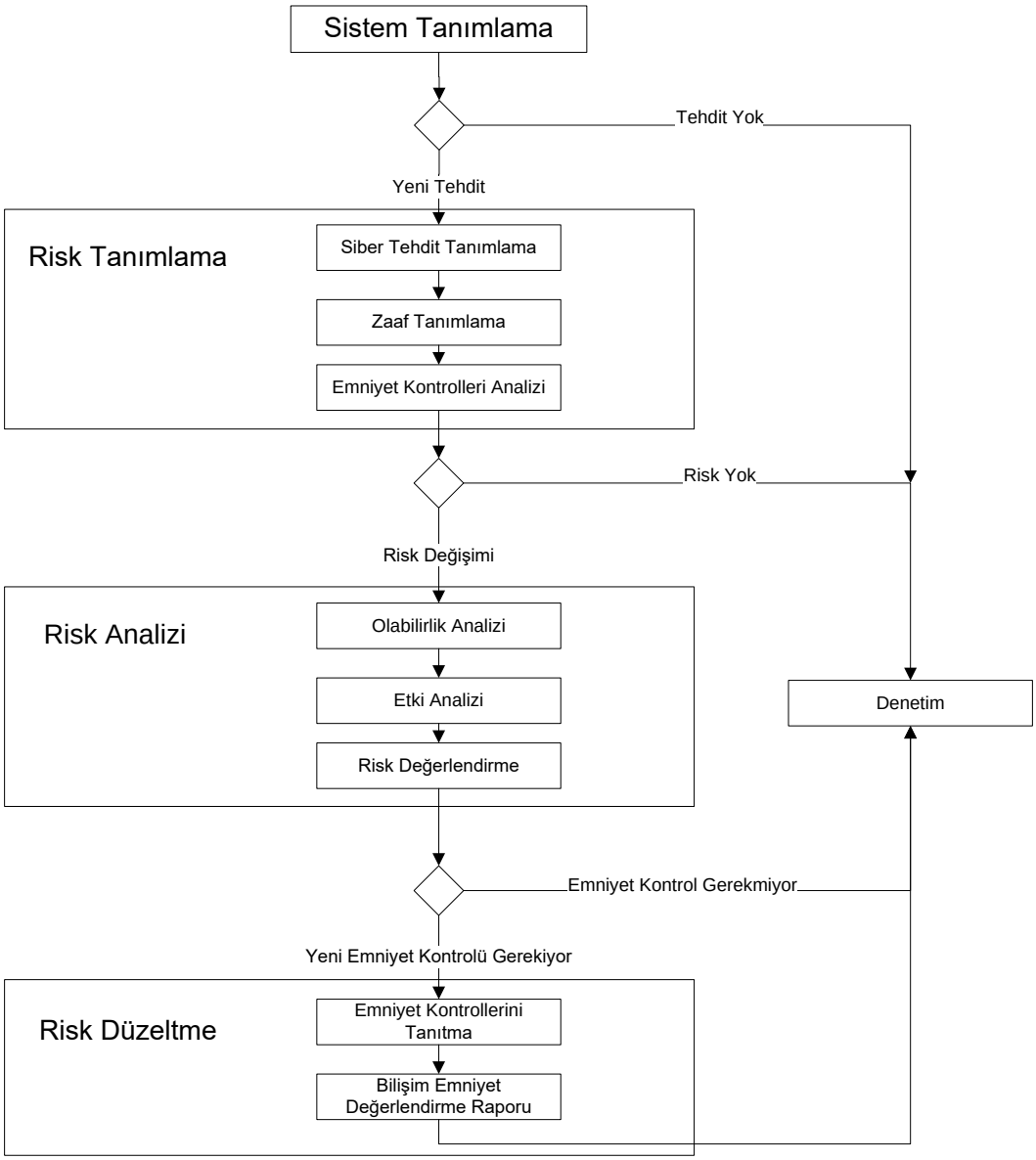
Risk değerlendirme ve yönetimi metodolojisinin temel basamakları:

- Çevre ve bağlam tanımı
- Tehdit tanımlama ve karakterizasyonu
- Zaaf değerlendirme
- Saldırı senaryolarına dikkatle hazırlanma
- Başarılı suiistimal olasılığı
- Risk seviyesinin belirlenmesi
- Önlem tanımı

Sistematik ve tutarlı risk analiz ve değerlendirmesi yapabilmek için mevcut standartlara uyan ve iyi tanımlanmış bir süreç kullanılmalıdır. Birçok risk değerlendirme ve yönetimi metodolojisi olgun bir hale getirilmiştir ve birçok kişi tarafından kullanılmaktadır ve bunların çoğu aynı kavram ve mantık üzere üretilmişlerdir. Bilgi emniyeti ve risk yönetimi konusunda mevcut standart ISO/IEC 27005'tir. Bununla birlikte tamamiyle ulusal bir risk değerlendirme ve stratejisi üretilebilir veya mevcutlara eklenebilir.

Sistemlerin değerlendirilmelerinin gereği, değerlendirmenin derinliği ve risk analizlerini güncelleme sıklığı, sistemin emniyet ve güvenlik özelliği açısından taşıdığı öneme bağlıdır. Yeni bir analiz yapıldığında veya var olan sisteme modifikasyon yapıldığında, en azından bir gözden geçirme yapıldığında, düşünülmelidir. Yeni ekipman, yazılım, prosedür veya operatör özelliklerinde belirgin majör bir değişiklik bu durumu bütünüyle karşılar. Potansiyel tehditlerin ve zaafların sayısı genellikle tek başına çalışan sistemden bağlaşımlı (enterkonnekte) çalışan bir sisteme geçişte artmaktadır.

Özel tehditlere karşı risk analizi yapmak pratik olmadığı durumlarda, en iyi uygulamalar ve iyi mühendislik prensipleri kullanılmalıdır. Aşağıda örnek siber risk değerlendirme algoritması görülmektedir: [13]



Şekil 6.2 : Bilişim emniyeti risk değerlendirme süreci.

6.3 Tehdidin Tanımı ve Özelliklerinin Belirlenmesi

Gelinen nokta bize şunu gösteriyor ki; artık saldırganların daha karmaşık saldırılar için daha az bilgili olmaları yeterli oluyor. Bilişim emniyeti programları, daha geniş spektrumdaki muhtemel saldırı senaryoları içeren bir değerlendirme seviyesini korumalıdır.

Büyük bilişim korsanlığı (hacker) olaylarında, endüstriyel sistemlerin zaafları üzerine olan yayınlar düzenli olarak görülmektedir. Bu yayınların, ilgili olaylar yaşandıktan veya test edildikten sonra yayınlandığı varsayılırsa, ne kadar dikkatli olmak gerektiği anlaşılır.

Bu nedenle, uygun bir kurulmuş destek ve kaynaklara sahip olduktan sonra, bir bilişim emniyeti programı geliştirmedeki ilk adımlar; saldırgan profilleri ve saldırı senaryoları temelinde potansiyel tehditleri anlamaya yoğunlaşmak olmalıdır. İlk adımda saldırganlar, motivasyonları ve potansiyel hedeflerini içeren bir saldırgan profil matrisi oluşturma olabilir. Bu matris daha sonra makul saldırı senaryoları üretmek için kullanılabilir.

6.3.1 Tasarıma esas tehditler

Tehdit seviyelerini belirlemede ve emniyet sistemi omurgası geliştirmede genel kullanılan araç, Tasarıma Esas Tehdit (TET)'dir. TET, dahili ve/veya harici potansiyel düşmanların nitelikleri ve özellikleri üzerine tanımlayıcı bir çalışmadır. Bir TET, güvenilir istihbarat kaynaklarından alınan bilgilerden türetilir fakat gerçekte olan tehditler anlamında değildir. Mevcut tehdit ortamı üzerine, TET tesisin maruz kalabileceği en geniş anlamda sorumlu olduğu tehditleri ifade eder. Devlet TET'yi, nükleer materyal ve tesisleri korumada kaynakların uygun konumlandırılması için yaptığı yönetmeliklerde kullanır.

Bu konuda kanaatler belirtilirken, hem tek başına saldırı hem de ortak bir saldırı senaryosu göz önüne alınmalıdır.

6.3.2 Saldırgan profilleri

Çizelge 6.1 ve 6.2 olabilecek saldırgan profillerinden bir kümeyi göstermektedir. Çizelge 6.1 iç tehditlere odaklı iken, Çizelge 6.2 dış tehdit odaklıdır. Profiller her tesis için ayrı adapte edilmelidir. Bundan dolayı her tesisin saldırgan matrisinin bütünsellik ve uyumluluğundan emin olmak için uygun bir bilgi toplama prosedürü gereklidir.

Çizelge 6.1 : Dahili tehditler.

Saldırgan	Kaynaklar	Zaman	Araçlar	Motivasyon
Gizli ajan	Sosyal mühendislik. Bazı seviyelerde sisteme erişim. Sistem dokümantasyon ve uzmanlığı	Değişir ama genellikle uzun saatleri alamaz	Mevcut erişim, programlama ve sistem mimarisi bilgisi:	Ticari bilgi, teknolojik sırlar, kişisel bilgi hırsızlığı
			Mevcut şifrelerin bilinmesi	Ekonomik kazanç (Rakiplere bilgi satma)
			Sistem arka kapılarından veya Trojanlar vasıtasıyla içeri girebilme becerisi	Şantaj
			Harici destek imkanı	
Kızgın/hoşnutsuz çalışan veya kullanıcı	Orta/kuvvetli kaynaklar	Değişir ama genellikle uzun saatleri alamaz	Mevcut erişim, programlama ve sistem mimarisi bilgisi.	İntikam, hasar, kaos
	Bazı seviyelerde sisteme erişim. Belli ticari konular ve işletme sistemlerinde sistem dokümantasyon ve uzmanlığı		Mevcut şifrelerin bilinmesi. Bazı yazılım kodlarını sokma imkanı	Ticari bilgi hırsızlığı. Diğer çalışanı/çalışanları veya işvereni utandırma. İmaj veya güven zedeleme

Çizelge 6.2 : Harici tehditler.

Saldırgan	Kaynaklar	Zaman	Araçlar	Motivasyon
Eğlence Korsanı	Çeşitli beceriler, genelde sınırlıdır. Dışa açık sistem dışındakiler hakkında sınırlı bilgi.	Çok zamanı vardır, ama genelde sabırlı değildir	Genel bilinen kodlar ve araçlar. Bazı araçlar geliştirmeleri de mümkündür	Eğlence, statü. Fırsat hedefleme. "Alçakta olan meyveleri istismar"
Nükleer Enerjiye Karşı Militan Muhalif	Sınırlı kaynaklar, fakat gizli kanallar ile destekleniyor olabilir.	Saldırılar belli zamanları hedef alıyor olabilir (Kutlamalar, seçimler vb.)	Bilgisayar becerileri vardır. Korsan komünitesinden destek alıyor olabilir. Sosyal mühendislik	Dünyayı kurtarma inancı. Kamuoyu düşüncesini etkileme. Ticari faaliyetleri engellemek
	Siber komünite araçlarına erişim. Dışa açık sistem dışındakiler hakkında sınırlı bilgi.	Çok zamanı vardır, sabırlıdır ve motivedir.		
Kızgın/hoşnutsuz olan eski çalışan veya kullanıcı	Eğer daha büyük bir grup tarafından desteklenmiyorsa sınırlı kaynaklar. Sistem dokümantasyonuna halen daha sahip olabilir. İptal edilmemiş eski erişimleri kullanabilir.	İlgili kişilere göre değişkendir	Mevcut şifrelerin bilinmesi. İptal edilmemiş eski erişimleri kullanabilir. Çalışıyor iken "arka kapılar" bırakmış olabilir. Sosyal mühendislik	İntikam, hasar, kaos. Ticari bilgi hırsızlığı. Diğer çalışanı/çalışanları veya işvereni utandırma.
	Tesis personeli ile eski bağlantılar			İmaj veya güven zedeleme

6.4 Risk Değerlendirmesinin Basitleştirilmiş Sonuçları

Çizelge 6.3, yalnızca bilgi amaçlı olarak, bir nükleer tesiste bulunabilecek sistemleri örneklerini içermektedir. Ele alınan sistemlerdeki başarılı saldırıların potansiyel etkileri, tesisle ilişkili etkileri ve uygun karşı önlemler için genel örnekleri tanımlar.

Çizelge 6.3 : Nükleer tesislerde tipik sistemler.

Sistem	Bilişim Sistemine Etkisi	Tesisteki Potansiyel Etkileri	Önerilen Karşı Önlemler
Reaktör koruma sistemi	Kritik yazılım ve veri emniyeti bütüncüllüğü kaybı Fonksiyon erişim kaybı	KRİTİK Saha emniyeti azalması, radyasyon	Seviye 1 Önlemleri
Proses kontrol sistemi	Kontrol yazılım ve verilerinin bütüncüllüğünün kaybı Fonksiyon erişim kaybı	YÜKSEK Saha operasyon azalması	Seviye 2 Önlemleri
Fiziksel erişim kontrol sistemi	Saha erişim sisteminin bütüncüllüğünün ve hizmette olmasının kaybı Site erişim bilgilerinin gizliliğinin kaybı	YÜKSEK Yetkisiz kişilere giriş izni verilmesi Yetkili kişilerin ilgili yerlere girişinin engellenmesi	Seviye 2 Önlemleri
Gözetleme Sistemi	Fiziksel erişim ve kontrol sistemlerine erişimin kolaylaştırılması	ORTA Yetki gerektiren girişlerin loglarının kaybedilmesi ve değiştirilmesi	Seviye 3 Önlemleri
İş izni ve iş emri sistemi	Veri ile sistem bütünselliğinin kaybı	ORTA Parçalarda yanlış eylemler Normal işletim ve bakımın kesilmesi	Seviye 4 Önlemleri
Belge Yönetim Sistemi	Veri gizliliğinin, erişilebilirliğin ve bütüncüllüğün kaybı	ORTA Daha şiddetli saldırılar için bilgi kullanımı	Seviye 4 Önlemleri
E-posta	Gizliliğinin, erişilebilirliğin ve bütüncüllüğün kaybı	DÜŞÜK İdari yükler. Günlük operasyonlar zorlaşır.	Seviye 5 Önlemleri

Risk değerlendirmenin temeli olan olabilirlik kavramı, bu çizelgede göz önünde bulundurulmamıştır. Başarılı saldırıların olabilirliği ve potansiyel sonuçları, ilgili tesise ve şartlarına göre değişir. Ek olarak, risk değerlendirilmesinde her bir sistem için gizlilik, bütünsellik ve erişilebilirlik için daha derin değerlendirmeler yapılmalıdır.

Tüm bunlarla birlikte belirlenen bazı riskler için ulusal bir kayıt tutulmalı, ulusal tehdit olarak algılanabilecek konularda devamlı olarak zaaflar ve tehditler gözetlenmelidir [14] .

7. NÜKLEER TESİSLER İÇİN ÖZEL HUSUSLAR

Nükleer endüstrinin özel şartlarından dolayı bilgisayar şebekeleri için düşünülen genel tedbirler dışında bazı hususlar da düşünülmelidir. Bu bölümde bu konulardan bahsedilmektedir.

7.1 Tesis Ömrü Aşamaları ve Çalışma Durumları

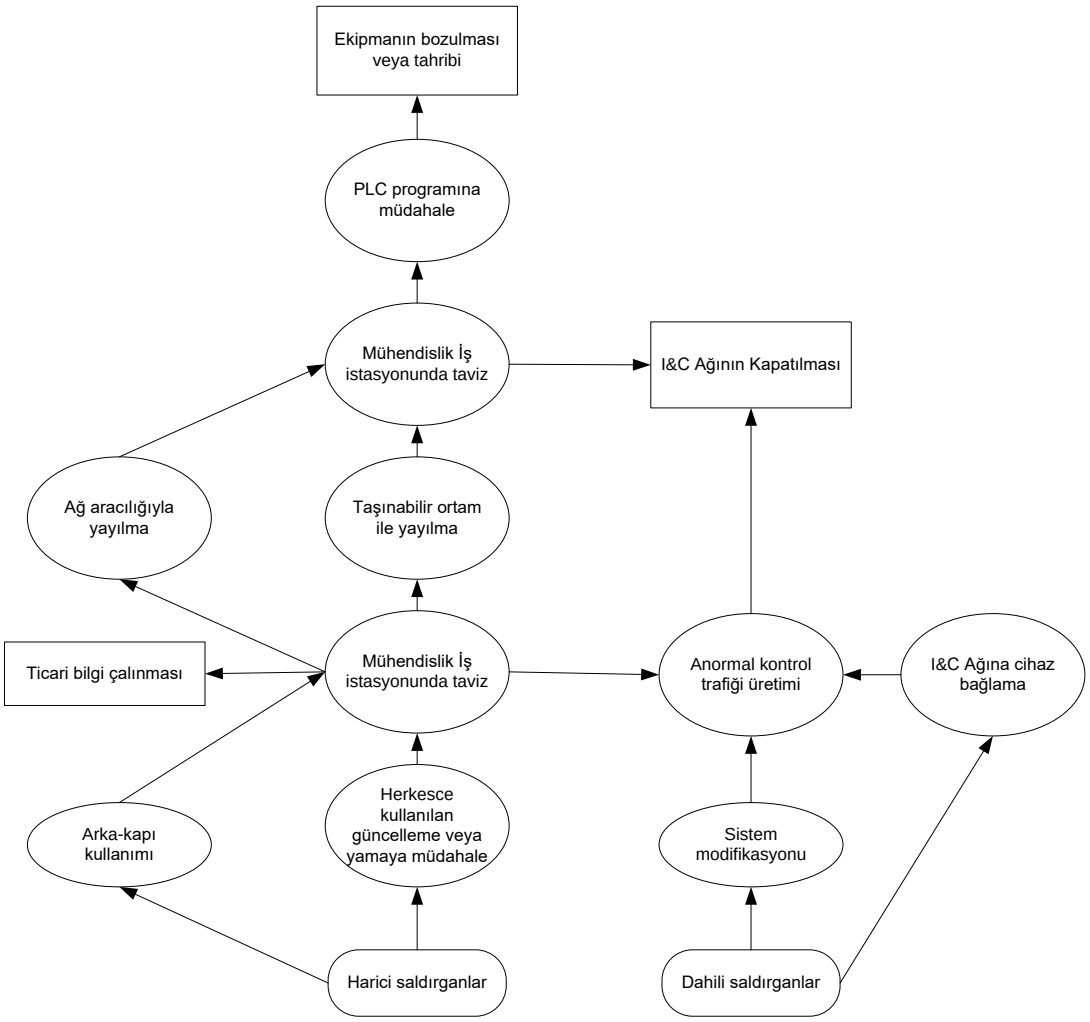
Nükleer tesislerin geniş bir çeşitlilikte tasarım ve işletme özellikleri vardır. Farklı tesis ömrü aşamaları ve çalışma durumları aşağıdakileri içerir:

- Tasarım, inşa ve hizmete alma
- Operasyonlar:
    - Güç operasyonları
    - Tesisin başlangıçta ayağa kaldırılması
    - Sıcak kapatış
    - Soğuk kapatış
    - Yakıt yükleme ve bakım
- Hizmetten çıkarma

Bu farklı aşamalar ve işletim durumları, farklı sistemler ve farklı işletim ortamları gerektirebilir. Mesela bakımın yoğun zamanları, ilave çalışan ve dışarıdan yüklenici ekip gerektirebilir. Böyle farklı durumlar BEP'nda hesaba alınmalıdır. Özellikle farklı fazlar, BEP'nda ciddi değişiklikleri gerektirebilir. Şekil 7.1'de şimdiye kadar olan saldırıların işleyiş algoritması şekillendirilmiştir: [15]

7.2 Bilişim Sistemleri ile Endüstriyel Kontrol Sistemleri Arasındaki Farklar

Nükleer saha operasyonlarını destekleyen bilişim sistemleri ve ağ mimarileri; konfigürasyon, mimarlık ve performans gereksinimleri açısından standart bilişim



Şekil 7.1 : Şimdiye kadar olan saldırıların işleyiş algoritması.

sistemleri değillerdir. Bu sistemler, Özelleştirilmiş Endüstriyel Kontrol Sistemleri olarak sınıflandırılabilir. Her ne kadar EKS'ler tamamiyle ara çözüm kurulumlarında standartlara bağlı anabilgisayar yapılarına doğru bir tekâmül içinde olsa da, halen daha BEP için göz önüne alınması gereken farklılıkları mevcuttur. EKS sistemlerinin, IT sistemlerine göre daha farklı güvenlik önlemleri ihtiyacı olduğu konular vardır. [16]

Takip eden tablo NIST'e (National Institute Standards and Technology – ABD Ulusal Standartlar ve Teknoloji Enstitüsü) göre farklılıkları göstermektedir.[17] Bunlar performans gereksinimleri, erişilebilirlik gereksinimleri, risk yönetim gereksinimleri, mimari güvenlik odağı, umulmadık sonuçlar, zaman-kritik etkileşim, sistem işletimi, kaynak tahditleri, iletişim, değişim yönetimi, destek yönetimi, parçaların kullanım ömrü, yedek parçalara erişim şeklindedir:

Çizelge 7.1 : Bilişim sistemleri ile endüstriyel kontrol sistemleri arasındaki farklar.

Kategori	Bilişim Teknoloji Sistemleri	Endüstriyel Kontrol Sistemi
Performans Gereksinimleri	Gerçek zamanlı değildir	Gerçek zamanlıdır
	Cevabın tutarlı bir şekilde ulaşması yeterlidir	Cevap/tepki tamamiyle zamansal hassaslığa haizdir
	Yüksek hız ister	Orta hız ister
	Gecikmenin olması kabul edilebilir	Gecikme asla kabul edilemez
Erişilebilirlik gereksinimleri	Yeniden başlatmak kabul edilebilir	Süreç erişilebilirliği açısından, yeniden başlatma kabul edilemez
	Erişilebilirlik kayıpları genellikle tolere edilebilir	Kapatmalar, önceden planlanarak yapılmalıdır
		Yüksek erişilebilirlik için, kurmadan önce birçok test gerekir
Risk Yönetim Gereksinimleri	Veri gizliliği ve bütüncüllüğü çok önemlidir.	İnsan emniyeti en önemlidir
	Hata toleransı daha az önemlidir	Hata toleransı çok önemlidir, anlık kesintilere bile tahammül yoktur.
	En büyük risk etkisi iş operasyonlarının gecikmesidir	En büyük risk etkileri, yönetmeliklere uymamak, insan, ekipman veya ürün kaybı
Mimari Güvenlik Odağı	Öncelikli odağı BT varlıklarının ve bunlar arası taşınan veya saklanan bilgilerin korunmasıdır	Öncelikli hedefi proses kontrolörlerinin korunmasıdır.
	Ana sunucu daha çok korumayı gereksinebilir	Ana sunucunun korunması da önemlidir
Umulmadık Sonuçlar	Güvenlik çözümleri genellikle BT etrafında şekillenir	Güvenlik araçlarının EKS tarafında bir ödüne sebebiyet vermediği test edilmelidir
Zaman kritik etkileşim	Acil durum etkileşimi daha az kritiktir	İnsan ve diğer varlıklara acil etkileşim kritiktir
	Gerektiğinde sıkı erişim kontrolü kurulabilir	EKS sistemine erişim sıkı kontrol edilmelidir
Sistem İşletimi	Sistemler tipik işletim sistemlerini kullanmak üzere tasarlanmışlardır	Güvenlik kısmının pek olmadığı farklı ve özel işletim sistemleri kullanırlar
	Otomatik kurma araçları ile sistem güncelleme mümkündür	Yazılım değişimleri dikkatlice ve yetkili servis aracılığı ile yapılmalıdır

Çizelge 7.1 (devam): Bilişim sistemleri ile endüstriyel kontrol sistemleri arasındaki farklar.

Kategori	Bilişim Teknoloji Sistemleri	Endüstriyel Kontrol Sistemi
Kaynak Tahditleri	Sistemler, gerektiğinde üçüncü taraftan gelecek güvenlik çözümlerini yüklemeye uygun kaynaklara sahiptir.	Sistemler ilgili endüstriyel prosesi desteklemek üzere tasarlanmışlardır. Güvenlik ile ilgili donanımsal vs. Bilişim kaynakları minimaldir.
İletişim	Standart haberleşme protokolleri	Birçok standart haberleşme protokolleri ve özel protokoller
	Kablolu ve bazen da kablosuz iletişim ortamları	Kablolu ve kablosuz ortam dışında çok farklı haberleşme ortamları (Mavidiş, Uydu vs.)
	Bilinen BT ağ yapıları	Karmaşık ağ yapıları
Değişim Yönetimi	İyi güvenlik politikaları ve prosedürleri ile otomatize edilmiş yazılım güncellemeleri	Çok dikkatli bir şekilde ve test ortamında öncelikle güncelleme yapılmalıdır
Destek Yönetimi	Farklı desteklere imkan tanır	Sadece ilgili üreticiden destek alınır
Parçaların kullanım ömrü	3-5 yıl	15-20 yıl
Yedek parçalara erişim	Genellikle kolay olur	Özel ithalat vb prosedürler gerektirir. Ayrıca değişim işlemi de zorlukla olur, ilgili parçalara sistem için erişmek zor olur, hassas işçilik gerektirir

7.2.1 İlave bağlantı talebi ve buna bağlı sonuçlar

EKS'ler için büyüyen bir başka ilgilenecek konu da, iş ve mühendislik sistemlerinin, operasyonel sistemlere bağlantı isteğidir. Şirket merkezlerinden, tasarımcılardan ve mühendislerden gelen gerçek-zamanlı verilere erişme talebi, sınırlandırılmış kontrol sistemleri ile şirket erişimi için sınırı olmayan veri ağının arabağlantı yerleri, ağa sızmak için bir geçit oluşturmaktadır.

Acil uzaktan işletim merkezi varlığı da başka bir özel mimari niteliktir. Bu acil işletim merkezleri, uzaktaki bir yerlerden gözetleme ve ana istasyonun kullanılamadığı durumlarda acil durum işletimi sağlarlar. Bu uzaktan erişim için elbette arada iletişim için kullanılan bir ortam olmaktadır. Bu ortam, ana sisteme giriş için potansiyel bir yol olmaktadır. Ayrıca, işleyebilen bu çift sistemin ikisi de emniyet gereksinimleri açısından göz önünde bulundurulmalıdır. Bir sistemdeki çöküş, diğer sisteme de giriş yolu açabilecektir.

Uzaktan analiz, bakım veya güncellemeler benzer zaaflar gösterebilir. Böyle bir ilave bağlantı için anlaşmadan evvel derinlemesine risk analizi yapılmalıdır.

7.3 Yazılım Güncellemeleri Üzerine Mülahazalar

Dünyadaki mevcut nükleer tesis ekipmanları için geçerli sertifikasyon, onaylama yönetmelikleri genel itibariyle sadece analog dünya varken geliştirilmiştir. Ve bunlar hemen zaman aşımına girmiyorlar. Bununla birlikte BT emniyet planları, düzenli güncellemeye uyan iyi örnekler, yazılım yamaları daha hızlı bir şekilde geçerliliğini yitiriyorlar.

İşte bundandır ki; dijital nükleer kontrol veya gözetleme sistemlerine yazılım yamaları ve güncellemelerinden gelen durumu da düşünmek önemlidir. En kötü durum senaryosunda, her yazılım modifikasyonu veya revizyonu, bir sistem değişimi olarak görülmelidir ve özel sistem onaylama ve hatta bazı kritik sistemlerin tekrar baştan sertifikalandırılmasına yol açabilir. Böyle bir yaklaşım hantal olacağından, yazılım yükseltme konusu geciktirilebilir. Bu etkileri sınırlamak için, böyle prosesleri olmayan normal bakımla, kritik sistemler için yeniden sertifikalandırma ve yeniden test gereken sistem modifikasyonları ayrılmalıdır. Bütün durumlarda bütün modifikasyonlar güvenlik, güvenlikle ilişkili sistemler, emniyet sistemleri için belirlenmiş prosedürlere uygun olarak yapılmalıdır.

7.4 Bilişim Sistemleri İçin Emniyetli Tasarım ve Özellikleri

Birçok proses kontrol, endüstriyel kontrol sistemi ve enstrümantasyonunun orijinal tasarım ve geliştirilmesinde bilişim emniyeti konusu öncelikli konu değildir. Gelişen süreçte; sistemler ve prosesler arası bağlantılar, internet aracılığıyla sıradan bilgisayarların neredeyse her yere erişebilir olmaları, korsanlık (hacking) gibi zararlı bilişim eylemlerinin artması, yeni ekipmanların alımında bilişim emniyetini temel bir gereksinim haline gelmiştir.

Sonuç olarak satın alma sözleşmelerinde bilişim emniyeti konusu da mutlaka yerini almalıdır. Bu kapsamda ISO 15048'den yararlanılabilir.

7.5 Üçüncül Taraf/Tedarikçi Erişim Kontrol Prosedürü

Üçüncül taraf ve tedarikçilerin erişim kontrollerinin de göz önüne alınması çok önemli bir konudur. Emniyet bölümü ile Satınalma bölümünün birbirleri ile yakın çalışarak, emniyet hükümlerinin bütün sözleşmelerde dâhil edilmiş olması sağlanmalıdır.

Sözleşmeler ve şartnameler, genelde üretici firmaların kendilerini korumak üzere ürettiği şablonlar üzerinden gidilerek yapılmaktadır. Bu nedenle ilgili sözleşmelerde tazminat, sonraki yönetimi zora koyacak maddeler, korunması gereken bilgiler, kontratın tehlikeye koyacağı varlıklar ve yetkisiz sonlandırma konuları da değerlendirilmelidir.

Yukarıdaki faktörler ışığında, müteahhit firma ile yakın ilişkide olmak, parça/sistem veya tesisi geliştirme, kurma ve işi teslim alma aşamalarında temel emniyet yönlerini sağlamak için önemlidir. Bakım ve test işlemleri esnasında harici cihazlar takılıyor olabilir [18]. Gerektiğinde müteahhit organizasyonun yönetim sisteminin emniyet sorunlarını yeterince giderdiğine ve önlemlerin sisteme uyumluluğuna dair denetim ve kontrol yapılmalıdır.

Bu tezi hazırlarken doğrusu, komplo teorisyenliği tarafımızın geliştiğini itiraf etmek gerekir. Fakat önemli bir kaynağın silah haline getirilme riski oldukça uyku kaçırıcı bir durumdur.

Üçüncül tarafın erişimi konusunda başka dikkat edilmesi gereken senaryo da, önce zayıf bir taşeron kullanılmasıdır. Bir ülke, kendi etki sahası içindeki başka bir

ülkeden saldırı gerçekleştirir. Hafif zarar veren bu saldırı için maruz kalan ülkeye, o büyük ülke, istenirse suçluların bulunması için destek verebileceğini ima etmiştir zaten. Büyük ülke, gelişen bu durum ile maruz kalan ülkenin bazı gizli verilerine erişim hakkı elde eder. Hatta bazı şüpheli durumlar bile o durumda tolerans sınırları içine sokulabilir. İşte asıl saldırı için gerekli tüm bilgilere ulaşılmıştır ve "büyük gün"e az kalmıştır!

8. BİLİŞİM EMNİYETİ İHTİYAÇLARINI BELİRLEMEK İÇİN BİR METODOLOJİ

Bir nükleer tesisteki bilişim emniyetini etkileyecek tehditleri tanımlama, kontrol etme, elimine etme veya minimize etme süreci, mevcut standartlara uygun olarak sistematik ve tutarlı bir şekilde kurulmalıdır. Bu bölümde özel bir metodoloji üretmek konusunda derinlemesine eğilmeye çalışılmıştır. Buradaki önerileri yapmak bütünüyle korumayı sağlayacaktır diye bir iddiada değiliz. Bununla birlikte daha güzel bir örnek olacağı kanaatindeyiz.

Genel olarak şunu ifade edebiliriz ki; herhangi bir bilişim sisteminin emniyet zaafları ve olası tehditleri belirlemek için öncelikle sistem işlevsellik ve teknik olarak analiz edilmeli ve korunması gereken faktörler belirlenmelidir. Sonra bu faktörlere ilişkin riskler belirlenmeli ve analiz edilmelidir.

Aşağıdaki paragraflarda EBIOS'tan bahsedilecektir. EBIOS, Fransızca "expression des besoins et identification des objectifs de sécurité" sözcüklerinin kısaltılmasından üretilmiştir ve "Emniyet hedeflerinin tanımlanması ve ihtiyaçların belirtilmesi" şeklinde tercüme edilebilir. Fransız Merkezi Bilgi Emniyeti Kurumu tarafından üretilmiştir. Fransa'daki nükleer tesislerin yoğun olarak enerji tedarikindeki yüksek yüzdesi, bu kurumun tedbirlerini merakımızı daha bir celp etmiştir.

EBIOS ile bilişim sistemlerinin emniyeti alanındaki riskleri değerlendirmek ve düzeltmek için, sözleşme yapan yetkilileri destekleyen, taslak belgeleri ve farkındalığı artırıcı araçları bulunan formal bir yaklaşım sağlama hedeflenmiştir.

8.1 EBIOS Metodunun Temelleri

8.1.1 Bağlam çalışması ve çerçeve tanımı

İlk adımımız bu çalışmanın teknik, ticari ve yönetmelik bağlamındaki ana hatlarını belirlemek olacaktır. Bir bilgi sistemi; temel unsurlar, işlevler ve işletmenin bilişim sistemine katma değer sağlayan bilgilere dayanır.

Mesela bir güç sahası soğutma sistemini gözetleme sistemi; önlemler, parametreler ve hesaplama sonuçları gibi farklı bilgilere dayanır. Bu hesaplamaları sağlayan değişik işlevler de göz önüne alınır. Temel unsurlar; donanım, yazılım, ağlar, organizasyonlar, insan kaynakları ve sahalar gibi farklı tipteki varlıklar ile bağlantılıdır. Mesela bir soğutma sisteminin özel bir pompa aktivasyonunu tetikleyen parametreleri ele alalım: Gözetleme bilgisayarlarına, işleyici yazılıma, operatörlere, soğuk kaynakların durumuna, sahanın durumuna, uygulanması gereken yönetmelik gibi konulara bağlıdır.

8.1.2 Hassasiyetin ifadesi

Doğru bir işleyişi garantilemek için her temel unsurun hassasiyeti belirtilmelidir. Bu ifade; erişilebilirlik, bütüncüllük, gizlilik gibi farklı emniyet kriterlerine bağlıdır. Eğer hassasiyet karşılanmazsa, işletmede nükleer emniyet ihlalleri, bozulmuş emniyet, aktivitelerin bozulması, müşteri güven kaybı veya mali kayıplar gibi değişik şekillerde etkisi olacaktır.

Örneğimize dönecek olursak; bu bilgi için erişilebilirlik ve bütüncüllük gereksinimi, materyal, çevre, personel hatta sahanın kullanılabilirliği açısından yüksek olmalıdır.

8.1.3 Tehdit çalışması

Her tesis kendi doğal çevresi, kültürü, imajı, çalışma sahası gibi açılardan, değişik tehditlere maruz kalırlar. Bir tehdit etmeni türü (doğal, insani, çevresel) ve sebebi (kazara veya kasdî) itibariyle karakterize edilebilir.

Tehdit etmenleri değişik saldırı metotları kullanırlar, bu nedenle tanımlanmaları gerekir. Bir saldırı metodu, ihlal edebileceği emniyet özellikleri ve tehdit etmenleri açısından karakterize edilir.

Örneğimize tekrar dönersek, bir nükleer güç sahası, birçok tehdit etmenini göz önüne almalıdır:

- İspiyonaj/Teknoloji hırsızlığı
- Kızmış çalışan/kullanıcı (içeriden ve dışarıdan)
- Eğlence için bilişim korsanlığı yapanlar
- Siber eylemciler

- Organize suç şebekeleri
- Dış düşman devlet
- Teröristler

Saldırı metotları olarak:

- Kulak misafirliği
- Ağa erişerek işletmeyi durdurma saldırıları
- Yazılım arka kapıları
- Kullanıcı isim ve şifre atakları (alfa numerik kombinasyonlar ile yapılan ataklar)

Her varlığın, tehdit faktörlerince kullanılabilecek, kendine göre bir zaafı olur. Burada nükleer güç üretim sahasının kendine has zaaflarını sıralamaya çalışırsak, aşağıdakileri belirtebiliriz:

- Tasarım ve geliştirme aşamasında saklanmış olası fonksiyonların varlığı (Yazılım)
- Değerlendirme aşamasından geçmemiş ekipman/parça kullanımı
- Sistem kaynak yazılımı tarafından yönlendirilebilen ağ (Ağ)
- Dolaylı erişim yolları ile binalara erişim (Yapı)
- Operatörün direktifler dışı kullanımı (Personel)
- Tasarım, kurulum ve işletim fazlarında emniyet önlemlerinin eksikliği

Aşağıda tehdit çalışmasında gözönüne alınması gereken öğeler ifade edilmiştir:

Şekil 8.1 : Tehdit çalışmasının adımları.

8.1.4 Emniyet hedeflerinin belirtilmesi

Şimdi temel unsurların tehdit etmenleri ve saldırı metotları ile nasıl etkileneceğini düşününüz: İşte risk budur.

Risk mümkün zararı ifade eder. Bu durum, temel unsurların dayandığı varlıkların zaaflarından yararlanmak için geliştirilen bir saldırı metodu ile bu unsurların tehdit etmenleri tarafından etkileneceği gerçeğinden çıkar.

Örnekte, yazılımsal bir tuzak ile ağla ilişkili sistem komutlarını üretmek ya da modifiye etme imkânından doğan ve materyal, çevre, personel güvenliği, tesis kullanılabilirlik ve kamu güveni üzerinde etkisi olan hassas bilginin ele geçirilmesi riski vardır.

Emniyet hedefleri temel itibariyle, varlıkların korundurulduğu risklerdeki zaafları kapsar. Aslında maruz kalınmayan şeye karşı korunma yoktur. Bununla birlikte risk potansiyeli arttıkça, emniyet hedeflerinin gücü de artırılmalıdır. Bu hedefler dolayısıyla, mükemmel şekilde adapte olmuş özellikler kümesini oluşturur.

Örnekteki nükleer güç üretim tesisi için emniyet hedeflerinden birisi de soğutma sistemi ağına ilişkin sistem komutlarının oluşturulması ve değiştirilmesine dair koruma olabilir.

8.1.5 Emniyet ihtiyaçlarını belirlemek

Yaklaşımın uygulanmasında görevli ekip, gerekli emniyet fonksiyonları için ihtiyaç duyulan tüm ve net özellikleri üretmelidir. Bundan sonra, fonksiyonel ihtiyaçlarca emniyet hedeflerinin kapsandığı gösterilmelidir.

Örnekteki ağa ilişkin sistem komutlarının değiştirilmesi ve üretilmesinden korunma maksatlı fonksiyonel ihtiyaçlar aşağıdakileri içerecektir:

- Normal işletim esnasında düzenli aralıklarla, doğru çalıştığını göstermek için bir dizi öz-deneme yapılır
- Fiziksel ve mantıksal erişim kontrolü

Nihai olarak, görevi üstlenen ekip varılması ve gösterilmesi gereken güven seviyesine izin veren güvence gereksinimlerini belirlemelidir.

Güvence gereksinimlerinden birisi de, gerekli direnç seviyesinde sistem emniyet fonksiyonlarının direnç analizini yürütmesi olabilir.

Bölümün başında ifade ettiğimiz gibi Fransa'da geliştirilmiş bu metodoloji, detaylı ve güzel bir örnek olarak ele alınabilir. Bununla birlikte her ülkenin kendi kanun ve yönetmelikler ve koşulları çerçevesinde daha güzel bir çalışmanın yapılması da

mümkün olabilir. Bu çalışma bütünüyle herşeyi kapsar iddiasında değiliz. Fakat bilişim emniyeti ihtiyaçlarını belirlemek için EBIOS'un değerlendirilmesi gereken iyi bir metodoloji olduğu kanaatindeyiz.

9. BİLİŞİM SİSTEMLERİNDE İNSAN HATASININ ROLÜ

Bu bölümde bilişim emniyeti konusunda beşeri performans sorunlarının etkileri incelenecektir. Bilhassa insan öğesinin beşeri performansından gelen etki ile özellikle saldırıya direnç, saldırıyı tanımak, önemli veri/hizmetleri tekrar sunmak, yeni çıkan tehditlere uyum sağlamak konularında organizasyonun kabiliyetini nasıl etkilediğini inceleyeceğiz. Emniyet gözetleme yazılımı, ağa sızmayı engelleme programları, daha güçlü yetkilendirme sistemleri ve daha güçlü şifreleme yöntemleri üzerine teknik çözümlerin geliştirilmesi için araştırmalar hararetle devam etmesine rağmen insan faktörünün sebep ve koruyucu önlem olarak ciddi etkisi unutulmaktadır. Birçok rapor bize bilişim emniyeti ihlallerinin asıl sebebini insan hatası olarak tanımlamaktadır. 2011 yılında yapılan tahminlere göre insan hatası kökenli ihlallerin oranı %60-80 arasındadır. Bu hataların çoğu, farkındalık ve işletim ve gözetlemede daha fazla titizlik üzerine yapılacak biraz daha yatırım ile engellenebilirdi.

Sistem/operasyonel devamlılık, bilişim emniyeti programının hedeflerinden biridir. Sistem devamlılığının öğeleri ise aşağıdakilerdir:

- Saldırıya sistem direnci
- Saldırıyı tanıma ve hasar tespiti
- Temel hizmet ve tam hizmet kurtarma
- Gelecekteki saldırılardan savunmak için sistem adaptasyonu ve tekâmülü

Çizelge 9.1 bu konuya odaklanarak, süreçlerdeki ve uygulamalardaki insan hatalarını kategorize etmeye çalışmaktadır. Beşeri hatalar hem sistem yöneticileri hem de kullanıcılar açısından ele alınmıştır. Bu listede çok ayrıntılı olmak niyet edilmemiştir, daha çok bu sistemlerin ve süreçlerin uygulanması ile ilgili insan etkileşimi düzeyini göstermek maksatlıdır.

Tablo insan faktörünün olumsuz etkileri odaklanmasına rağmen, insan faktörünün olumlu tarafları da unutulmamalıdır. Bazen en zayıf halka insan olmasına rağmen, an

Çizelge 9.1 : Genel beşeri hatalar.

Süreç/Uygulama	İnsan Hatası
Saldırıya Direnç	
Erişim sınırlama (Sistem Yönetimi)	Dosyalara yanlış izin vermeler
	Gereksiz servislerin açık bırakılması
	Saldırıya karşı zayıf portların açık bırakılması
	Fiziksel erişim izni
	Ekran koruyucuların şifresiz kullanımı
	Sistem yamalarının eklenmemesi
	Yama eklemenin merkezi olmaması
	Zararlı yazılımların indirilip yüklenmesi
Şifre üretimi/kullanımı	Şifrelerin yazılması
	Zayıf şifreler
	Varsayılan şifrelerin kullanılması
	Şifrenin başkasına söylenmesi
	Şifre kullanmama
	Güvenli ve güvensiz sistemlerde aynı şifrenin kullanılması
Saldırı ve hasarın tanımlanması	
Ağa sızmayı algılama sistemleri	Yanlış konfigürasyon - kural serisi
	Sistem güncellemelerin yapılmaması
	Log kayıtlarının incelenmesi konusunda ihtiyat olmaması
Logların denetimi	Log günlüklerinin incelenmesinde özen eksikliği
	Çoklu log kayıtlarındaki trendlerin farkında olmamak
Sistem kurtarma	
Yedekleme ve geri yükleme	Yedeklememek
	Belli aralıklarla yedeklememek
	Yanlış konfigürasyon
	Yedekleme ortamına fiziksel hasara sebebiyet vermek
	Ortamları fiziksel olarak yok etme
	Kazara veri silme
	Yedekleme ortamlarının güvenliğin ve korumanın olmadığı yerlerde saklanması
	Bozulmuş ortam kullanımı
	Kartuş vesair ortamları yanlış etiketleme
	Kurtarma prosedürlerini test etmeme
	Kritik sistem bilgilerinin çoklu kopyalarının olmaması
	Yedekleme ortamının tesis dışında bir yerlerde de saklanmaması
Yeni tehditlere adaptasyon	
Kurum prosedürleri	Kurum politikasını bilmeme
	Kurum politikası ihlali
	Kurumun geri kurtarma politikasının olmaması
	Geçerliliği eskimiş politika kullanımı
	Politika/prosedürlerin işlerliği testinin yapılmaması
	Politikanın uygulanması konusunda zorlamanın olmaması

gelir ve bir operatör sistemin kapanmasını engeller. Teknoloji hiçbir zaman komple bir çözüm olmayacaktır. Çalışanlar her zaman derinlemesine savunma stratejisinin katmanlarından olacaktır. İncelemeler düzenli olarak, önde gelen emniyet sorununun, bilişim emniyeti farkındalık ve eğitiminin eksikliğinden kaynaklandığını tespit etmektedir.

Bilişim emniyeti açısından ve sistem devamlılığı için çalışanların aşağıdakileri tamamiyle kazanmış olmaları gereklidir:

- Genel bilişim emniyeti planındaki rollerinin önemini güçlü bir şekilde anlamaları
- Kendi sorumlulukları tarafındaki gerekli bilişim emniyeti bilgisi ve becerisi
- Etkin bir emniyet kültürünün kendileri ile başladığının anlaşılması [19]

10. NÜKLEER TESİSLERDEKİ SİSTEMLERE YÖNELİK SALDIRI SENARYOLARI

Bölüm 6.3'te de belirtildiği üzere, korunmamız gereken bilgisayar tabanlı saldırıların yapıları ve şekilleri farklı olabilmektedir. Yüksek seviyede sonuçlara sebep olan saldırılar aşağıdaki gibi olabilir:

- Bilgiye yetkisiz erişim veya yetkililerin erişimini engelleme (Gizlilik kaybı)
- Veri, yazılım, donanım vs.'nin yetkisiz kişilerce modifikasyonu (Bütüncüllük kaybı)
- Veri iletim hatlarının blokajı veya sistemlerin kapatılması (Erişim kaybı)

10.1 Saldırı Senaryoları

Saldırı senaryoları oluştururken, birçok ihtimal arasından bir tanesi farklılaşabilir. Nükleer tesise aşağıdaki amaçlar ile saldırılabilir:

- Tesis sabotajı veya nükleer madde çalınması için sonradan koordineli saldırı yapma
- İnsan ve çevre güvenliğini tehlikeye atma
- Başka bir yere saldırmak için giriş yeri yapma
- Kafa karışıklığı ve korkuya sebep olma
- Bir suç örgütüne para karşılığı yapmak
- Piyasada aşırı hareketlenmeye sebep olarak bazı piyasa oyuncularına fayda sağlamak

Saldırının gaye hedeflerine bağlı olarak saldırgan, farklı sistem zaaflarını suiistimal edecektir. Bu saldırılar aşağıdakilere sebep olur:

- Bilgiye yetkisiz erişim (Gizlilik kaybı)
- Bilgi, yazılım, donanım vs.'nin tutulması ve değiştirilmesi (Bütünsellik kaybı)

- Veri iletim hatlarının blokajı ve/veya sistemlerin kapatılması (Erişim kaybı)
- Veri haberleşme sistemlerine veya bilgisayarlara yetkisiz sızma (Güvenilirlik kaybı)

Bütün bu yönler, bilişim sistemlerinin işlevselliği üzerinde büyük etkiler ve sonuçlara sebep olabilir, bunlar da tesisin güvenlik ve emniyetinin doğrudan veya dolaylı olarak tehlikeye sebep olabilirler. Saldırı senaryoları hazırlanırken, teknolojik trendler ve saldırı teknolojilerine erişim kolaylığı da göz önünde bulundurulmalıdır.

Mevcut durumdaki saldırılardaki araçlardan bahsetmek gerekirse; Botnet (robot network), robot ağ adı verilen programları ifade eder [20]. Botnet, bir veya birden fazla bilgisayarı uzaktan kontrol altına alan programa verilen isimdir. Bu tip saldırı altında olan bilgisayar kullanıcıları genellikle donanıma zararlı bir yazılım yüklendiğinden haberdar olmazlar. DoS (Denial of Service) saldırısı, "hizmet engelleme" kelimelerinin birleşimiyle tanımlanan bir eylemdir. DoS saldırılarında kullanılan yazılımlar, belirli ağ kaynaklarına yetkili erişimi engelleyen programlardır. Mantık bombası (logic bomb), belli bir programın içine kasıtlı olarak zararlı bir kod yerleştirilmesi işlemine verilen isimdir. Mantık bombası genellikle hedef alınan bilgisayar veya ağlardaki bilgileri yok etmek veya kulanılamaz duruma getirmek için kullanılır. Truva atı (Trojan horse), kullanıcıların çalıştırmak istedikleri program gibi davranan yazılımlara verilen isimdir. Mantık bombasına benzer bir sistemle çalışır. Virüs, hedef bilgisayar veya ağlara zarar vermek için yazılan bir uygulamadır. Solucan (worm) ise kendi kendisini yayabilen virüs programıdır. Bu programlar genel olarak, ağlara karşı DoS saldırısı gerçekleştirmek veya virüs sokmak için "arka kapı" (backdoor) olarak bilinen sistem açıkları kurmak için kullanılırlar.

Bilişim saldırılarına karşı koruyucu önlemler geliştirirken, saldırıların doğasını, saldırının veya saldırganın nerelere saldıracağını anlamak çok önemlidir. Aşağıdaki örnekler sadece tehditleri daha çok anladıkça, organizasyonları için gerektiğinde emniyet önlemlerini düzeltmeye teşvik maksatlıdır. Senaryolar her ne kadar fiktif olsa da, başka endüstri alanlarında yaşanmış olaylardan esinlenmiştir.

İyi yönetilmiş bir bilişim saldırısında birkaç faz olur. Bu fazlar aşağıdakileri içerir:

- Hedef belirleme

- Keşif
- Sisteme erişim
- Saldırının gerçekleştirilmesi
- Arkada iz bırakmamak

Yeri gelmişken “Sıfırıncı Gün” saldırısından da bahsetmek gerekir. Kimsenin daha önceden bilmediği bir zaafın saldırgan tarafından bulunup saldırılması eylemine “Sıfırıncı Gün Saldırısı” denmektedir. Birkaç sebepten dolayı saldırganlar bu tip saldırıları daha çok önemserler: [21]

- Henüz kimse farkında olmadığından yüzlerce site bu şekilde ele geçirilebilir veya zarar verilebilir.
- Bu zaaf bilgisini yüksek rakamlara satabilir.
- Bilgisayar korsanları komünitesindeki şanlarını artırmaya güçlü bir sebep olur.

10.2 Örnek Senaryolar

Aşağıda örnek olarak üç senaryo verilmiştir:

10.2.1 Senaryo 1 - Zarar verici bir eylemi desteklemek için bilgi toplamak

Saldırının hedefi; sonraki bir saldırıya hazırlık olması için, sadece yetkililerin girebildiği alanlara fiziksel erişim sağlamak.

Buradaki hedef kişi, yetkileri tanımlayan ve erişim izinlerini yöneten kişidir. Sınırlı alanlara fiziksel erişim hakkı elde etmek, hem kart yöneticisinin bilgisayarının hem de erişim şifresi sisteminin zayıflamasını içerecektir. Saldırgan, ekipman parçalarını sağlayan müteahhit gibi davranmayı seçer.

Saldırıyı destekleyecek bilgileri toplama sürecindeki olası hedefler:

- Olası gasp ya da 'sosyal mühendislik' olayları için personelin bilgileri
- Erişim kontrol sisteminin tasarım dokümantasyonu
- Sahanın emniyet sisteminin veya ilgili benzer bir sistemin politika ve mühendislik planları

- İşletmenin zamansal planları, takvimi: Günlük işler, vardiya değişimleri, kim ne zaman çalışıyor, kimler tatilde, önemli değişiklikler ne zaman yapılacak
- Tedarikçilerin listesi ve sahada ne zaman çalıştıkları
- Ekipman ve parça envanteri
- Şifre ile erişim kontrol önlemleri
- Erişim kontrolünün idari ve teknik önlemleri
- Yazılım geliştirici ve mevcut proje bilgisi
- Ağ mimarisi
- İletişim mimarisi

Bunları toplamak için potansiyel metotları:

a. Sosyal mühendislik (İstenilen bilgiyi hissettirmeden alma)

Sosyal mühendislik teknikleri arasında aşağıdakileri zikredebiliriz: [22]

- Güven uyandırmak
- Yardımcı olmak
- E-posta ile saldırı (phishing: E-posta ile kişi kandırılarak şifre, parola gibi bilgileri edinilir)
- İstenilen şeyin acil yapılması gerektiğine ikna. Eğer karşıdaki kişi şunları istiyorsa sosyal mühendislik yapıyor olabilir:
  - İsteğinin yerine getirilmemesi durumunda kötü şeyler olacağının vurgulanması
  - Sıradışı taleplerde bulunulması
  - Soru sorduğunuzda rahatsız olması
  - Yeni yetkilendirildiğini söylemesi
  - Bildiğiniz konu ve isimleri ard arda söylemesi
  - İltifat etmesi veya kur yapması

Sosyal mühendisliğin zararlarını azaltmak için aşağıdaki başlıklar değerlendirilebilir: [23]

- Sorumluluğun yayılımı: Eğer hedefe onların kendi hareketlerinden sadece sorumlu olmadıklarına inandırılırsa, sosyal mühendisin ricasına uygun hareket ederler. Sosyal mühendisler çeşitli faktörlerin de yardımı ile oluşturdukları durumda, kişisel sorumluluk konusunu şaşırtma ile o kadar sulandırırlar ki bir karar vermeye zorlarlar. Sosyal mühendisler karar verme sürecinde diğer çalışanların isimlerini kullanırlar, ya da yüksek seviyeden yetkilendirilmiş bir eylem olduğunu diğer bir çalışanın ağzı ile iddia ederler.
- Göze girme şansı: Hedef eğer bir rica ile razı olan birisi ise, başarılı olma şansı yüksektir. Bir rakip olarak onu yönlendirmede bu çok büyük bir avantaj sağlar, ya da bilinmeyene göre yardım verir, sıcak bayan sesini kullanarak telefon aracılığı ile iletişime girerler. Sistem korsanları topluluğuna teknoloji ile içli-dışlı insanlar olarak toplumsal ilişkilerde çoğu zaman beceriksiz insanlar topluluğu olarak bakılır. Nitekim bu kanı da doğrudur. Sosyal mühendisler, etkilemenin yüksek hiçbir formunu kullanmadan bilgi elde ederler.
- İlişkilere Güvenmek: Çoğu zaman, sosyal mühendisler belirledikleri kurban ile iyi güvenilir bir ilişki için beklerler ve o zaman bu güveni sömürürler. Bunu takip eden zamanlarda ufak küçük etkileşimlerle ilişkiye girer ve doğal seyir içinde problem ortaya çıkar ve sosyal mühendis büyük hamlesini yapar. Böylece karşı taraftan şans verilmiş olur.
- Ahlâkî görev: Hedefi dışarıdan ahlakî olarak davranmaya cesaretlendirmek ya da başarı şansı için ahlaki hareket arttırmayı sağlamak. Bu durum için hedef olan kişi ya da organizasyondan bilgilerin sömürülerek alınmasını gerektiren bir iştir. Hedef eğer karşıdakine uymanın yanlış olduğuna inanırsa karşıdakini sorgulamanın hoş olmadığını hissederse, başarı şansı artmış demektir.
- Suçluluk: Eğer mümkünse çoğu insan suçluluk hissinde olmaktan sakınır. Sosyal mühendisler çoğu zaman, psikodrama üstatlarıdır. Öyle bir mizansen hazırlarlar ki insanın yüreği sızlar, empati ve duygudaşlık meydana getirirler. Eğer suçluluk duygusunu ortadan kaldıracak bir

bağışta bulunurlarsa hedef bundan çok fazla memnun olacaktır. Rica edilen bilginin yerine getirilmeyeceğine inanarak, belirleyici problemlerin rica eden kişi tarafından sık sık yeterli ağırlıkta tartılıp denge içinde iyilik olsun diye yapılmasını sağlarlar.

- Künye: Sosyal mühendisin hüneri ile daha çok hedef tanımlanır ve bilgiye erişilir. Sosyal mühendisler iletişim anında daha çok zekice bir araya getirilmiş öncelikli, temelli girişimlerle bağlantı kurmaya çalışırlar.
- Faydalı olmaya istekli olmak: Sosyal mühendisler diğer insanlara yardım etmeden zevk alanlara güvenerek eylemlerini yürütürler. Kahramanımız karşı kişiden ya bir giriş hakkı ister ya da bir hesaba giriş için yardım etmesini ister. Sosyal mühendisler ayrıca birçok bireyin zayıf reddetme düzeyini bilerek ve işin uzmanına danışmanın dayanılmaz cazibesine sırtlarını dayayarak işlerini yaparlar.
- Birbirine göre ayarlama: Hedef ile en az çatışma en iyisidir. Sosyal mühendisler genellikle ortamın gerektirdiği ses tonu ile zekice ve sabırlı sunuş yaparlar. Emir gibi, bir şey sipariş eder gibi, sinirli ve baş belası gibi kazanmak adına nadiren çalışırlar. Sosyal mühendis kahramanları genellikle direkt rica edenler, uydurma durum, kişisel ikna gibi kategorileri kullanırlar.
- Direkt rica edenler: muhtemelen en basit metottur ve başarı için en son olan yoldur. Bir işe basitçe girişildiğinde sorulan bilgidir. Direkt rica genellikle meydan okumadır ve genellikle ret edilir. Başarı şansı düşük olduğundan nadiren tercih edilir.
- Uydurma durum: Bir şey veya bir organizasyonun özelliğine göre elde edilen bilgilerle yapılan üretilen bir durum, bir kriz veya özel bir an ile ilgili olarak bu durumdan faydalanmadır. Kriz durumları anlık yardım içerir, sosyal mühendisler hedefin güvenini arttırıcı durumun gerekliliği ve yardım edilme ile ilgili ortam oluştururlar. Sosyal mühendislerin taktikleri gerçek üzerine kurulu olsa da şunu unutmamak gerekir ki; kahramanlar gerçek tabanlı şeylere ihtiyaç duymaz, sadece ortalama gerekli şeylerle çalışırlar.

- Kişisel ikna: Kişisel olarak yardım yapmayı isteyen bununla ilgili istekli insan gibi davranırlar. Amaçları kuvvetli uyum değildir, gönüllü-uyumlu insan anlayışına ulaşmaya çalışmaktır. Birçok bilişim teknolojisi emniyetinde çalışan insan gerekli bilgilerden yoksun bulunmaktadır. Bu işle uğraşanlara yönelik bilgi emniyeti farkındalığı programı uygulanmalıdır. Son kullanıcı kılavuzu, emniyet öngörüleri ve emniyet bilgileri olmalıdır. Çalışanların, sosyal mühendis riski ile ilgili eğitimi bu saldırılara karşı kurumların savunma aracıdır. Sosyal mühendisler psikoloji üzerine kurulu ve sosyal hainliklere dayalı yeni hileler ile bizimle paylaşımda bulunurlar. Bu çok özel saldırı metodunun farkındalığı için özel süreçlerde eğitim ve çalışma gerektirir.

b. Halka açık internet arama motorları

c. Çöplük dalışı: Atık konteynırına atılmış kartlara atıklar içinden ulaşmak veya tamamiyle silindiği sanılan bilgilere erişmek

d. War-driving: Genellikle bir mobil araç içinden kablosuz sistemlerdeki TCP/IP portlarını tarayarak içeriye sızmaya uygun zayıflıkta olanı bulmak

e. Flash bellek, DVD, harici disk gibi ortamlar ile yazılım yükleme

f. Erişim şifrelerine kulak kabartmak (sesli veya görüntülü takip veya akıllı telefonlara yüklenecek korsan yazılımlar ile)

Saldırının içeriğinde aşağıdakiler olabilir:

- Geçiş kartının ve şifresinin edinimi
- Var olan kartın duplikasyonu veya çalınması
- Kart makinesine yeni kart basımı için erişim
- Yeni personel işe giriş kaydı yapılması
- Daha yeni işten çıkarılmış personelin kimliğini kullanmak
- İstenilen düzeyde erişim hakkı verilmesi

Saldırgan, kart ve şifresini edindikten sonra, hiç şüphe uyandırmadan, yedek parça tedarikçisi müteahhit firma elemanı olarak tesise girebilir.

10.2.2 Senaryo 2 – Bir veya daha fazla bilgisayarı çalışamaz hale getirmek veya işlevselliklerini kısıtlamak

Saldırının hedefi; nükleer enerji üretim tesisisin sabotajı ve hemen tekrar üretime başlamasını engellemek.

Bu örnekte, bir müteahhit kapatma periyodu esnasında, besleme suyu kontrol sisteminde test yapmaktadır. Müteahhit, sistemi uzaktan gözetlemek ve test etmek için uzaktan erişim sistemi kurar. Yüklenici işi teslim ettikten sonra uzaktan erişim sistemi yanlışlıkla halen daha çalışır olarak kalır.

Saldırgan, yüklenici firmanın daha önce tesiste çalıştığını belirler ve bilgi toplama için ana hedef olarak belirler. Bu aşamada yüklenici firmanın ofisine bir e-posta ile "phishing" saldırısı yapar ve idari kontrolü ele geçirir. Böylelikle saldırgan yüklenicinin ağını ele geçirir, planlarını bulur ve henüz daha aktif olan TCP/IP portunu öğrenir.

İşte tam bu aşamada saldırgan, DoS (Denial of Service) saldırısı ile ağa çekebileceğinin üstünde bir trafik üreterek, besleme suyu kontrol sisteminin çalışmasını durdurmaya hazırdır. DoS saldırısı, kullanıcıların sunuculara erişmesini engelleyen saldırıdır. Sunucuya durdurulamaz bir sel gibi veri gönderilerek, sunucunun bütün kaynakları meşgul edilir ve sunucu hiçbir kullanıcıya hizmet veremez hale gelir.

DDoS (Distributed Denial of Service) ise dağınık kaynaklardan eş zamanlı yapılan yapılan DoS saldırısıdır [24]. Emniyet duvarı, Bantgenişliği Dengeleyici, Uygulama Sunucuları gibi saniyede milyon isteği bile cevaplayan cihazları servis dışı bıraktırabilirler. Örneğimizdeki bu sistem minimal trafik yükü çekmek üzere tasarlanmıştır. Dolayısı ile kısa süreli bir DoS saldırısı sistemini çökertebilir.

Saldırı neticesinde besleme suyu sisteminin vermez olması, işletmenin manuel olarak kapatılması ile sonuçlanır. Besleme suyu kontrol sisteminin arızası hemen çözülebilen bir sorun değildir, araştırma-soruşturma neticesinde tesis tekrar işletime açılabilir.

10.2.3 Senaryo 3 – Koordineli bir saldırı hazırlığı için bilgisayar sistemini zayıflatma

Saldırı hedefi – nükleer maddelerin tesis depolama alanları arasındaki taşınması esnasında çalınması.

Bilgisayar saldırısı ile envanter ve takip sistemi değiştirilecek ve çalınan materyalin kaybı gizlenecek. Keşif ve istihbarat toplama, depolama alanları arası radyoaktif madde yüklemelerini takip ve izleme sürecini tanımlar. Bu işlem, parçalar ve içeriklerin listelendiği RFIDlerin etiketlenmesini de içerir.

Plan içerideki adamlarının yardımı ile, taşıma esnasında materyalin kaçırılmasıdır. Saldırı üç aşamayı içerir:

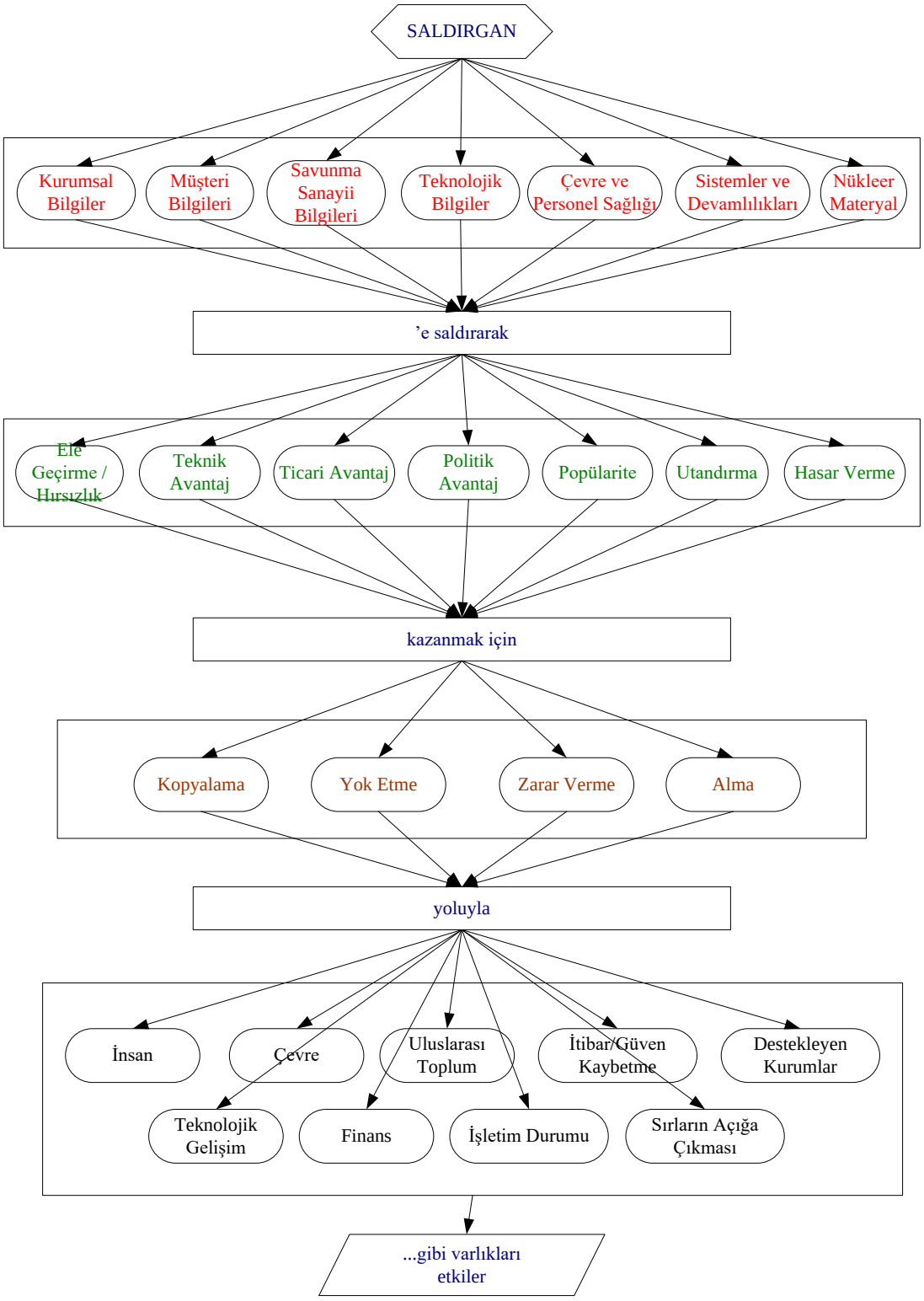
1. Taşıma esnasında yolun kesilmesi
2. Yüklenmiş radyoaktif maddeden görece az olanın alınması
3. RFID'nin tekrar yüklenerek, eksik hali ile olan miktarı gösterir duruma getirilmesi
4. Envanter takip sisteminde değişiklik yaparak, çalınan kısımdan hariç kalan kısmın, başlangıçta olan tüm kısım olarak işlenmesi

Bu bilişim saldırısının odağı envanter veritabanına ve işlem kayıtları bilgisayar ağı erişimidir. Saldırgan erişimi bir kere sağladı mı, network haritasını çıkarır, iletişim protokollerini belirler ve artık saldırıyı yönetir.

Saldırı senaryoları üretmek için takip eden şekilden veya çizelgeden kombinasyonlar ile yararlanılabilir. [25]

Bu çizelgede iki ana konu belirlendi; "Tehdit aktör analizi" ve "Etki analizi". Burada tehdit eden aktörün kazanımları ve amaçları neler olabileceği iredelendi. Benzer çalışma etki analizi için de yapıldı. Risk üzere olan varlıklar belirlendi ve potansiyel etkileri düşünüldü. Bütün bunların farklı kombinasyonları ile değişik saldırı senaryoları üretilebilir.

Her sütundan bir veya birden fazla öğe de seçilerek senaryo üretilebilir. Mesela Çizelge 10.2'deki gibi olsun ve buna uygun bir senaryomuz Senaryo 4 gibi olabilir:



Şekil 10.1 : Saldırı senaryo üretim algoritması.

Çizelge 10.1 : Senaryo seçimi.

Tehdit Aktör Analizi		Etki Analizi	
Kazanımı	Amacı	Risk Üzere Olan Varlık	Potansiyel Etkisi
Ele geçirme/Hırsızlık	Kopyalama	Teknolojik Bilgiler	İşletim Durumu
Ticari Avantaj	Yok etme	Kurumsal Bilgiler	İtibar/Güven Yitirilmesi
Teknik Avantaj	Zarar verme	Müşteri Bilgileri	Sırların Açığa Çıkması
Politik Avantaj	Alma	Savunma Sanayi ile İlgili Bilgiler	İnsanlar
Popülarite		Çevre ve Personel Sağlığı	Çevre
Utandırma		Sistemler ve Devamlılıkları	Destekleyen Kurumlar
Hasar Verme		Nükleer Materyal	Uluslararası Toplum
			Finans
			Teknolojik Gelişim

Çizelge 10.2 : Örnek senaryo seçimi -1.

Tehdit Aktör Analizi		Etki Analizi	
Kazanımı	Amacı	Risk Üzere Olan Varlık	Potansiyel Etkisi
Ele geçirme/Hırsızlık	Kopyalama	Teknolojik Bilgiler	İşletim Durumu
Ticari Avantaj	Yok etme	Kurumsal Bilgiler	İtibar/Güven Yitirilmesi
Teknik Avantaj	Zarar verme	Müşteri Bilgileri	Sırların Açığa Çıkması
Politik Avantaj	Alma	Savunma Sanayi ile İlgili Bilgiler	İnsanlar
Popülarite		Çevre ve Personel Sağlığı	Çevre
Utandırma		Sistemler ve Devamlılıkları	Destekleyen Kurumlar
Hasar Verme		Nükleer Materyal	Uluslararası Toplum
			Finans
			Teknolojik Gelişim

10.2.4 Senaryo 4 – Sosyal mühendislik ile dahili bilgisayar ağına erişmek

Saldırı hedefi – nükleer enerji tesisinin güvenilirliğini kamuoyunda sarsacak bir sansasyon oluşturmak.

Nükleer enerji karşıtı bir grup, Akkuyu'daki Santral'i kısa süreli dahi olsa durdurmak ister. Bu başarılırsa, olay farklı şekilde anlatılacak, ve "Sızıntı oldu, ama saklıyorlar. Bölge insanı ve çevre tehlikede!" gibi haberler sosyal medya aracılığı ile yayılacaktır.

Hedef olarak, üretim bölümünde çalışan ve bazı EKS'lerine erişimi olan, asosyal tipteki bir mühendistir. Bu yetkili mühendis, bazen sisteme sanal özel ağ bağlantısı üzerinden bağlanarak, özellikle tatilde olduğu zamanlarda destek verebilmektedir. Mühendisin internetteki izlerinden, nelerden hoşlandığı tespit edilir. Onun tam da kafasına uygun özelliklerde bir sanal tip oluşturulur. Bu sanal tip o mühendise sosyal medya üzerinden arkadaş olur ve ona bazı eğlenceli internet linkleri gönderir. O linklerde bazı arka kapı oluşturacak veya solucan tarzı virüsleri içerecek yeni üretilmiş programlar vardır. Yeni ve özel üretildiğinden antivirüs programının orta seviye hassasiyeti onu yakalamaz. Üst seviye hassasiyette yakalanıyor olmasından ise bu asosyal mühendis şüphelenmez, çünkü samimi arkadaşından gelen bir linktendir.

Mühendis sanal özel ağ bağlantısı ile EKS'ye bağlandığında, saldırgan grup kendilerine mühendisin bütün bağlanma bilgilerini kopyalarlar. Artık saldırı için her şey yeterlidir. Kendilerini o mühendis gibi sisteme tanıtarak erişirler. Sonrasında ise ilgili sistemi durdururlar. Bu durdurma diğer sistemleri de etkilediğinden reaktörün kısa süreliğine durdurulması zorunluluğu ortaya çıkar. Hatayı yapan mühendis gibi görülür, ama yapan aktivistlerdir.

Senaryo üretimi konusunda başka bir örnek verelim. Takip eden sayfadaki gibi olsun:

Çizelge 10.3 : Örnek senaryo seçimi -2.

Tehdit Aktör Analizi		Etki Analizi	
Kazanımı	Amacı	Risk Üzere Olan Varlık	Potansiyel Etkisi
Ele geçirme/Hırsızlık	Kopyalama	Teknolojik Bilgiler	İşletim Durumu
Ticari Avantaj	Yok etme	Kurumsal Bilgiler	İtibar/Güven Yitirilmesi
Teknik Avantaj	Zarar verme	Müşteri Bilgileri	Sırların Açığa Çıkması
Politik Avantaj	Alma	Savunma Sanayi ile İlgili Bilgiler	İnsanlar
Popülarite		Çevre ve Personel Sağlığı	Çevre
Utandırma		Sistemler ve Devamlılıkları	Destekleyen Kurumlar
Hasar Verme		Nükleer Materyal	Uluslararası Toplum
			Finans
			Teknolojik Gelişim

10.2.5 Senaryo 5 – İçeriden birisinin yanlış veri enjeksiyonu ile EKS'yi yanıltmak

Saldırı hedefi – radyoaktif sızıntıya sebep olacak bir eylemi başlatmak, geliştirmek

Teknisyenlerden birisinin görevi, dijital veri toplanamayan analog bir ölçme cihazından verileri girmektir. Bu kişi işe alındığı zaman itibariyle emniyet araştırmalarından olumlu bir rapor alınmasına rağmen, ilerleyen zamanlarda oluşan kumar borcundan dolayı ciddi finansal sıkıntı içerisindedir. Zaten muhalif güçlerin takibinde olan bu kişi ağa düşmüş ve artık para ve sığınma hakkı karşılığında eylemi yapmaya hazırdır.

Yapması gereken şeyler çok basittir. Reaktördeki soğutucu sistemin bağlı olduğu kontrol sistemine yanlış veri girişi yapılacaktır [26]. EKS'ler kendilerine sensörler, uzak terminaller gibi elemanlardan aldıkları bilgiler ile otomatik karar verirler ve işlerler. Devreye bu yanlış veri sokulması ile sistem gerektiği gibi çalışmayacak ve reaktör yakıtının aşırı ısınması sonucu sistem emniyet sınırlarının üstünde bir radyoaktif yayınıma sebep olacaktır.

Gerekli kontrol sistemlerinin tekrar doğru mantık işlemeleri veya manuel olarak sistem kapatılır. Sızıntı olmadan engellenmesi durumunda çevre ve insan sağlığı belki korunmuş olur, ama finansal olarak, reaktörün kapatılmasından dolayı zararda olunacağı kesindir.

11. SONUÇ VE ÖNERİLER

Nükleer tesislerin bilişim emniyetini sağlamak, tasarım ve kurulum aşamasından başlayarak, işletimi süresince ve olası kapatılma süreci de dâhil olmak üzere hayati önem arz etmektedir.

2000'li yıllar ile gelişen ve yaygınlaşan bilişim ve internet teknolojileri ile uzak sistemlerin yakın olması sağlanmıştır. Bununla birlikte endüstriyel kontrol sistemlerinin daha akıllı olmasının getirdiği sayısal olma ve haberleşebilme durumu, birçok avantajının yanında nükleer tesisleri tehlikelere daha açık bir hale getirmiştir.

Bu çalışmamızda yaptığımız öneriler IAEA tarafından sunulan öneriler çerçevesinde, daha genişletilmiş bir halidir. Nükleer tesislerin bilişim emniyeti konusu, her seviyedeki paydaşlar açısından öncelikli olmalı ve bu açıdan bir kültür oluşmalı, değerlendirme ve eylemler doğru planlamalar dâhilinde yapılmalı, düzenli olarak bu planlar ve eylemler gözden geçirilmeli, tesis çalışanları için peryodik olarak eğitim programları geliştirilmelidir. İnsan faktörünün olduğu her yerde emniyet açıkları olabileceği gibi, nükleer tesisler için de bu geçerlidir. Kademeli bir savunma stratejisi geliştirilmeli ve var olmayan tehditlere karşı da teyakkuz halinde olunmalıdır.

Kademeli emniyet sistemi oluşturulurken, benzer özellik, emniyet hassasiyeti olan bölümler aynı mantıksal alanda toplanmalı ve o seviyede benzer kurallar işletilmelidir. EKS'lerin yönetildiği alandan iletişim tek yönlü olmalı, daha az güvenli yerden erişim olmamalıdır.

Kanun ve yönetmelik koyucu ve standart belirleyici kurumlar, genel emniyet ve bilişim emniyeti konularında ilgili kuralları belirlerken, nükleer tesislere olabilecek etkileri de göz önüne almalıdırlar.

Bilişim emniyeti tesisin her aşamasında önemlidir. Bu nedenle her aşaması için ayrı ayrı senaryolar üretilmeli ve bunlara karşı alınacak tedbirler belirlenerek, gerek ilgili yönetmelikler ve sözleşmeler ile uygulanıldığından emin olunmalı, denetlenmeli ve kontrol edilmeli, gerekse kurum kültürünün bir parçası haline yönetim tarafından getirilmelidir.

Önlenebilecek saldırıların kötü sonuçlarını yaşamak zorunda değiliz. Saldırı senaryolarına önceden çalışarak ve derinlemesine savunma yöntemi uygulanması ile, muhtemel saldırıları ciddi bir şekilde engellemek mümkündür.

KAYNAKLAR

[1] **Url-1** <http://www.taek.gov.tr/nukleer-guvenlik/nukleer-guvenlik/479-nukleer-güvenlik.html> Alındığı tarih: 23.11.2015

[2] **Url-2** <http://www.taek.gov.tr/nukleer-guvenlik/nukleer-guvenlik/426-nukleer-guvenlik.html> Alındığı tarih: 23.11.2015

[3] **IAEA Nuclear Security Series No. 17**. Technical Guidance Reference Manual, Computer Security at Nuclear Facilities. International Atomic Energy Agency, Viyana, 2011. Sayfa 1-88

[4] **Lindsay J**., (2013) Stuxnet and the Limits of Cyber Warfare, *Security Studies Dergisi, Sayı 22, Sayfa 365*

[5] **Vulnerability of nuclear plants to attack.** *Wikipedia.* Erişim tarihi:15.11.2015 <https://en.wikipedia.org/wiki/Vulnerability_of_nuclear_plants_to_attack>

[6] **Karaçor M., Keleş K**. (2007) Otomasyon Sistemlerinin Bileşenleri. "Otomasyon Sistemlerinin Bileşenleri", VI. Otomasyon Sempozyumu, (23-25 Mayıs 2007 Samsun)

[7] **Url-3** <http://www.bbc.com/news/technology-12465688> Erişim tarihi: 10.10.2015 Stuxnet Virus Targets and Spread Revealed,. BBC News. 15 February 2011.

[8] **Url-4** <http://www.reuters.com/article/2011/04/17/iran-nuclear-stuxnet-idUSPOM73176820110417#jt4kKxjdvGg5cWC3.97 > Erişim tarihi:15.11.2015.

[9] **Kesler B.,** (2011) The Vulnerability of Nuclear Facilities to Cyber Attack, *Strategic Insights Dergisi, Volume 10, Issue 1*, sayfa 15

[10] **Kim D.**, (2014) Cyber security issues imposed on nuclear power plants, *Annals of Nuclear Energy Dergisi Sayı 65* Sayfa 141

[11] **Son H., Kim S**., (2014), Defense–in–Depth Architecture of Server Systems for the Improvement of Cyber Security, *International Journal of Security and Its Applications Cilt.8, No.3* Sayfa 262

[12] **TS ISO/IEC 15408-1:2010-03** Bilgi teknolojisi - Emniyet teknikleri - Bilgi Teknolojisi (BT) emniyeti için değerlendirme kriterleri, sayfa 22

[13] **Park Jaekwan, Park Jeyun, Kim Y.**,(2013) A graded approach to cyber security in a research reactor facility, *Progress in Nuclear Energy Dergisi, Sayı 65,* Sayfa 87

[14] **Falessi N., Gavrila R., Klejnstrup M., Moulinos K.** (2012) National Cyber Security Strategies, Practical Guide on Development and Execution ENISA Sayfa 10.

[15] **Woogeun A., Manhyun C., Byung-Gıl M., Jungtaek S.,** (2015) Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs**,** *International Journal of Distributed Sensor Networks, Volume 2015, Article ID 836258*, Sayfa 9

[16] **Kang Y., Chong K.,** (2010), Development of Cyber Security Assessment Methodology for the Instrumentation & Control Systems in Nuclear Power Plants, *Journal of Korea Academia-Industrial cooperation Society Vol. 11, No. 9* Sayfa 3453

[17] **Stouffer K., Falco J., Scarfone K.,** (2011) Guide to Industrial Control Systems (ICS) Security,. *NIST Special Publication 800-82* Sayfa 28.

[18] **Song J., Lee J., Park G, Kwon K., Lee D., Lee C**., (2013) An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants, *Nuclear Engineering And Technology, Cilt 45 No.5, Ekim 2013 Sayısı*, Sayfa 639

[19] **Lochthofen A., Sommer D**., (2015) Implementation of computer security at nuclear facilities in Germany, *Progress in Nuclear Energy Dergisi, Sayı 84,* Sayfa 105

[20] **Çelik Ş.**, (2013) Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Cilt:15, Sayı:1,* Sayfa: 141, 142

[21] **Url-5** <http://learn-how-to-hack.net/> The Hacker's Underground e-book, Sayfa 56, Erişim tarihi: 28.09.2015

[22] **Url-6** <http://www.turkhackteam.org/sosyal-muhendislik/580412-sosyal-muhendislik-kisa-konu-ozetleri.html> Erişim tarihi:08.11.2015

[23] **Url-7** <http://www.turkhackteam.org/sosyal-muhendislik/577677-sm-ye-karsi-savunmayi-artirma.html> Erişim tarihi: 08.11.2015

[24] **Url-8** <http://www.digitalattackmap.com/understanding-ddos/> Erişim tarihi: 15.11.2015

[25]**Green I**., (2013). “Extreme Cyber Scenario Plannıng & Attack Tree Analysis”, RSA Conference 2013, GRC-T17 nolu oturumdaki sunumundan esinlenilmiştir.

[26]**Serpanos D., Shrobe H.,** (2015). “False Data Injection Attacks on Industrial Control Systems”, RSA Conference 2015, CIN-W08 nolu oturumdaki sunumundan esinlenilmiştir.

ÖZGEÇMİŞ

Ad Soyad **: GÖKHAN AKAR**

Doğum Yeri ve Tarihi **:** ANKARA, 1973

E-Posta **:** gokhanakar@gmail.com

ÖĞRENİM DURUMU:

- **Lisans** **:**1996, İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Elektronik ve Haberleşme Mühendisliği Bölümü

MESLEKİ DENEYİM VE ÖDÜLLER:

İş hayatında bilişim teknolojileri üzerine çalıştı. 1998 yılında Türkiye'deki ilk CCDA (Cisco Certified Design Asscociate) ünvanını alanlardandır. Gerek aktif gerekse pasif ağ cihaz ve elemanları ile birçok bilgisayar ağı kurdu. Yine Türkiye'deki ilk FTTB (Fiber To The Building – Binaya kadar fiber optik) projesinin beyni olarak projenin yöneticiliğini yaptı ve başarı ile ilgili telekom firmasına teslim etti. İstanbul'daki belediye, valilik, güvenlik kurumlarının deprem halinde sürekliliği devam edecek iç haberleşmeleri için fiber optik altyapısının proje müdürlüğünü yaptı. Özellikle MAN (Metropolitan Area Networks) pasif altyapısı konusunda derin bilgi ve tecrübeye sahiptir. Farklı yurtdışı firmalarının Türkiye mümessili olarak çalıştı. Evli ve iki çocuk babasıdır.