1. AMAÇ

Bu politika, **Uşak Üniversitesi Bilgi İşlem Dairesi Başkanlığı** içerisinde geliştirilen sistemlerin temel yöntemlerini belirlemek amacıyla yazılmıştır.

2. KAPSAM

Uşak Üniversitesi Bilgi İşlem Dairesi Başkanlığı içerisinde geliştirilen sistemlerdir.

3. SORUMLULUK

Bu politikadan Uşak Üniversitesi Bilgi İşlem Dairesi Başkanlığı sorumludur.

4.UYGULAMA

Güvenli bilgi sistemleri oluşturmada yardımcı olmak amacıyla, NIST (Ulusal Standartlar ve Teknoloji Enstitüsü – USA) sistem güvenliği için bir dizi mühendislik ilkeleri derledi. Bu ilkeler, bilişim teknolojileri güvenlik önlemlerinin tasarlanması, geliştirilmesi ve uygulanmasına yönelik daha tutarlı ve yapılandırılmış bir yaklaşımın uygulanabileceği bir altyapı sağlamaktadır.

Bahsi geçen ilkelerin temel odağı teknik kontrollerin uygulanması iken yine bu ilkeler, etkililiğin sağlanması için bir sistem güvenliği tasarısının aynı zamanda politika, işlemsel süreçler ile kullanıcı farkındalığı ve eğitimi gibi teknik olmayan konuları da göz önünde bulundurularak oluşturulması gerektiği gerçeğini vurgulamaktadır.

Tercihen, burada sunulan ilkeler bir programın başlangıcında kullanılıp daha sonra sistemin her aşamasında uygulanabilir. Ancak bu ilkeler, hâlihazırda kullanılan bilgi sistemlerinin güvenlik durumunun doğrulanması ya da onaylanmasında da yardımcı bir görev üstlenmektedir. Kısa ve öz olan bu ilkeler, sistem döngüsündeki politikaları geliştirmek amacıyla tüm kuruluşlarca kullanılabilir.

Bu kılavuz, tüm sistemlere uygulanabilen genel güvenli mühendislik ilkelerini sunmaktadır (sürekli değişen bilgi sistem güvenlik ortamından dolayı her zaman mümkün olmasa da). Her bir ilke, her sistemin yaşam döngüsü boyunca dikkatlice düşünülmelidir.

Burada sunulan ilkeler, aşağıdakiler tarafından kullanılabilir:

- İşlevsel gerekliliklerin geliştirilmesi ve değerlendirilmesi ya da kuruluşlardaki bilgi sistemlerinin işletilmesi aşamasındaki kullanıcılar,
- Bir bilgi sistemini tasarlama, uygulama ya da değiştirme aşamasındaki Sistem Mühendisleri ve Mimarları,
- Sistem döngüsündeki tüm evrelerde Bilişim Teknolojileri Uzmanları,
- Sistem döngüsündeki tüm aşamalarda yeterli güvenlik önlemlerinin ele alındığından emin olmak için Program Yöneticileri ve Bilgi Güvenliği Yöneticileri.

Güvenli mühendislik ilkeleri uygulaması öncelikle geliştirme altındaki yeni bilgi sistemlerinde ya da büyük güncellemeler geçirmekte olan sitemlerde hedeflenmektedir ve tüm sistem geliştirme döngüsüne dahil edilmelidir. Eski bilgi sistemleri için kuruluşlar, sistem güncellemeleri ve değişiklikleri ile mümkün mertebe sistemdeki donanım, yazılım ve aygıtların mevcut durumuna da güvenli mühendislik ilkelerini uygulamalıdır.

GÜVENLİK TEMELİ

1. **Tasarımın "temeli" olarak tam bir güvenlik politikası oluşturun.**

Güvenlik politikası, bir bilgi sistemi tasarlarken geliştirilecek önemli bir belgedir. Güvenlik politikası, kuruluşun genel bir politika raporu olarak ifade edilen bilgi güvenliğine karşı esas bağlılığı ile başlar, daha sonra sistem tasarımı ya da güvenlik çözümünün her aşamasına uygulanır. Politika, sistemin desteklemesi gereken güvenlik amaçlarını (gizlilik, bütünlük, erişilebilirlik, izlenebilirlik ve güvence) tanımlar ve bu amaçlar Bilgi Teknolojileri güvenlik mimarisi tasarımında kullanılan prosedürleri, standartları ve kontrolleri yönlendirir. Aynı zamanda, kritik varlıkların, algılanan tehditlerin ve güvenlikle ilgili rol ve yükümlülüklerin belirlenmesini gerektirir.

2. **Güvenlik'i tüm sistemin ayrılmaz bir parçası olarak düşünün.**

Güvenlik konusu, bilgi sistemi tasarımında dikkate alınmalı ve sistem döngüsüne tam anlamıyla entegre edilmelidir. Bir sistem geliştirildikten sonra güvenlik önlemlerini düzgünce ve başarılı bir şekilde sürece dahil etmenin hem zor hem de maliyetli bir durum olduğunu tecrübelerimiz sonucunda görmüş bulunmaktayız; bu nedenle, güvenlik eylemleri tüm yeni bilgi sistemlerinin tasarım aşamasında ve mümkünse tüm eski sistemlerin değiştirilmesi ve işleyişi aşamalarında da uygulanmalıdır. Bu ilke aynı zamanda, güvenlik politikaları oluşturma, ortaya çıkan güvenlik gerekliliklerini yorumlama ve güvenlik ürünlerinin değerlendirilmesi ile sistemin planlanıp düzenlenmesi, tasarlanması, uygulanması ve elden çıkarılması aşamasına katılımı da içermektedir.

3. **İlgili güvenlik politikaları tarafından yürütülen fiziksel ve mantıksal güvenlik sınırlarının tarifini açıkça yapın.**

Bilgi teknolojisi fiziksel ve mantıksal lokasyonlarda bulunur ve sınırlar bunlar arasında yer alır. Nelerin dış etkenlerden korunması gerektiğinin anlaşılması, gerekli miktarda koruyucu önlemlerin en etkili olacakları yerlerde uygulandığını garanti edebilir.

Bazı durumlarda sınır, bir fiziksel lokasyonla ilgili insanlar, bilgi ve bilgi teknolojisi tarafından tanımlanır. Ancak bu, tek bir lokasyonda dahi bazıları kamuya açık bilgileri, bazısı da hassas ve gizli bilgileri kapsayan birçok farklı güvenlik politikaları olabileceği gerçeğini göz ardı eder. Diğer durumlarda sınır, fiziksel sınırları geçebilen birtakım özel bilgi ve bilgi teknolojisini yöneten bir güvenlik politikası tarafından tanımlanır. Bu sorunu daha da karmaşık hale getiren şey çoğu zaman tek bir makinenin ya da sunucun hem kamuya açık hem de hassas bilgileri içerebilmesidir. Sonuç olarak, çoklu güvenlik politikaları bir makineye

ya da bir sisteme uygulanabilir. Bu nedenle bir bilgi sistemi geliştirirken güvenlik sınırları, ilgili sistem dokümantasyonunda ve güvenlik politikalarında göz önünde bulundurulmalı ve anlatılmalıdır.

4. **Geliştiricilerin nasıl güvenli bir yazılım geliştirileceği hakkında eğitildiğinden emin olun.**

Sistemi geliştirmeden önce geliştiricilerin güvenli yazılımın tasarımı, geliştirilmesi, konfigürasyon kontrolü, entegrasyonu ve ölçülmesi konularında yeterince eğitilmiş olduğundan emin olun.

RİSK ODAKLI

5. **Riski kabul edilebilir bir seviyeye indirin.**

Risk, (1) belirli bir tehdit kaynağının (kasıtlı ya da kasıtsız olarak ortaya çıkan) belirli bir bilgi sistemi zafiyetine neden olma olasılığı ve (2) bu ihtimal gerçekleşirse kurumsal işlemler, varlıklar ya da bireyler üzerinde ortaya çıkacak olumsuz etkilerin kombinasyonu olarak tanımlanır.

Tüm risklerin ortadan kaldırılması, uygun maliyetli bir işlem değildir. Her önerilen kontrol için bir maliyet-kazanç analizi yapılmalıdır. Bazı durumlarda, daha güvenli bir sistemin faydaları doğrudan ya da dolaylı maliyetleri ortaya koymayabilir. Kazançlar yalnızca maddi kayıpların önlenmesinden fazlasıdır; örneğin, kontroller kamu güveni ve inancını sürdürmek için zorunlu olabilir. Doğrudan maliyetler, satın alma ve sunulan teknolojiyi yükleme maliyetiyken dolaylı maliyetler, azaltılmış sistem performansı ve ek eğitimlerdir. Amaç, görev/iş risklerini kabul edilebilir bir seviyeye düşürerek görev/iş yeterliliklerini arttırmaktır. (6.İlkeyle ilgilidir.)

6. **Harici sistemlerin güvenli olmadığını varsayın.**

Bilgi alanı terimi, bilgi kaynaklarının erişim kontrolü, ihtiyaçlar ve gerekli koruma seviyelerine göre paylaştırılması uygulamasından doğmaktadır. Kuruluşlar, bu paylaştırmayı güçlendirmek ve bilgi alanları arasında yetkilendirilmiş bilginin istemli akışını sağlamak için özel ölçümler uygulamaktadır. Bir bilgi alanının sınırı, o alanın güvenlik çevre uzunluğunu temsil eder.

Harici alan, kontrolünüz dışında olan kısımdır. Genel anlamda harici sistemlerin güvenli olmadığı düşünülmelidir. Harici alan "güvenilir" olarak addedilene kadar sistem mühendisleri, mimarlar ve Bilişim Teknolojileri uzmanları harici sistemin güvenlik ölçümlerinin, güvenilir bir dahili sisteminkinden ve sistemin buna uygun olarak gösterdiği tasarım özelliklerinden farklı olduğunu varsaymalıdırlar.

7. **Azalan risk ve artan maliyetler ile işlemsel verimliliğin diğer alanlarındaki azalma arasındaki potansiyel değiş-tokuşları saptayın.**

Belirtilen güvenlik gerekliliklerini karşılamak için sistem tasarımcısı, mimarı ya da güvenlik uygulayıcısının tüm rakip işlemsel ihtiyaçları saptaması ve bunların üzerine eğilmesi gerekecektir. Diğer işlemsel gerekliliklerden dolayı güvenlik hedeflerini değiştirmek ya da ayarlamak gerekebilir. Güvenlik hedeflerini değiştirirken ya da ayarlarken daha büyük bir risk ve maliyeti kabul etmek kaçınılmaz olabilir. Karar merciiler bu değiş-tokuşları mümkün olduğunca çabuk saptadıklarında ve bunlarla ilgilendiklerinde daha rahat olacak ve daha etkili sistemler oluşturabileceklerdir. (4. İlke ile ilgilidir.)

8. Kurumsal güvenlik hedeflerini karşılamak için özel olarak belirlenmiş sistem güvenlik ölçümlerini uygulayın.

Genellikle Bilişim Teknolojileri önlemleri, kuruluşun kendi ihtiyaçlarına göre özel olarak belirlenir. Ek işlem gereklilikleri ve rehberlik gibi birçok etken düşünüldüğünde temel konu görev ve işlerin Bilişim Teknolojileri güvenliği ile ilgili olumsuz etkilerden korunmasıdır. Bilişim Teknolojileri güvenlik ihtiyaçları tek tip olmadığından sistem tasarımcıları ve güvenlik uygulayıcıları, diğer harici ağlara ve dahili alt alanlara bağlanırken güven seviyesini göz önünde bulundurmalıdır. Her sistemin benzersiz olduğunun farkında olmak kullanılmak üzere katmanlı bir güvenlik stratejisine (yalnızca en kritik alanlarda daha az kritik sistemleri ve daha yüksek güvenlik çözümlerini korumak için daha az maliyetle daha düşük güvenlik çözümleri uygulamak) imkân oluşturur.

9. İşleme, iletme ve depolama sürecinde bilgiyi koruyun.

Verinin yetkisiz olarak değiştirilmesi ya da bozulması, bilginin ifşası ve iletirken veriye erişimin reddedilmesi gibi riskler, depolanan ya da işlenen veri ile ilgili risklerle birlikte ele alınmalıdır. Bu nedenle sistem mühendisleri, mimarlar ve Bilişim Teknolojileri uzmanları; bilgi işlenirken, iletilirken ve depolanırken bütünlüğü, gizliliği ve uygulama yazılımı da dahil olmak üzere verinin erişilebilirliğini korumak için güvenlik önlemlerini uygulamalıdır.

10. Yeterli güvenliği sağlamak için özel ürünleri dikkate alın.

Tasarımcılar, bazı durumlarda tamamıyla ticari amaçlı kullanıma hazır (COTS) ürünlerden oluşturulmuş sistemlerle güvenlik hedeflerine ulaşmanın mümkün olmayabileceğinin farkında olmalıdırlar. Böylesi durumlarda COTS'ları COTS olmayan mekanizmalarla çoğaltmak gerekli olabilir.

11. Tüm olası "saldırı"lara karşı korunun.

Güvenlik kontrolleri tasarlanırken birçok "saldırı" türü ele alınmalıdır. Kabul edilemez riskle sonuçlanan türler hafifletilmelidir. Bazı "saldırı" türü örnekleri şunlardır: pasif izleyen, aktif ağ saldırıları, içeriden gerçekleşen istismarlar, fiziksel erişim ya da yakınlık gerektiren saldırılar ve yazılım geliştirme ve/veya dağıtma sırasında izinsiz erişim girişlerinin ve zararlı kodların eklenmesi.

KULLANIM KOLAYLIĞI

12. Taşınabilirlik ve birlikte işlerlik ile ilgili açık standartlar üzerinde temel bir güvenlik oluşturun.

Çoğu kuruluş, görev ve işlemleri sürdürmek için dağıtılmış bilgi sistemlerine güvenmektedir. Bu sistemler, bilgiyi hem kendi kuruluşları içinde hem de diğer kuruluşlara dağıtırlar. Böylesi çevrelerde etkili olabilecek güvenlik yeterliliklerini karşılamak amacıyla güvenlik programı tasarımcıları birlikte işlerlik ve taşınabilirlik ilkelerini donanım, yazılım ve uygulama denemeleri de dahil olmak üzere tüm güvenlik ölçümlerine dahil etmek için ellerinden geleni yapmalıdırlar.

13. Güvenlik gerekliliklerini geliştirirken ortak bir dil kullanın.

Güvenlik gerekliliklerini geliştirirken ortak dil kullanımı, kuruluşların ortak test ortamlarında değerlendirilen güvenlik ürünlerini ve özelliklerini değerlendirmesine ve karşılaştırmasına olanak sağlamaktadır. Bir "ortak" değerlendirme süreci, ortak gerekliliklere ya da kriterlere dayandığında güven seviyesi, ürün güvenlik işlevlerinin kuruluşun güvenlik gereklilikleri ile uyum sağladığını garanti edecek seviyeye kadar getirilebilir. The Common Criteria (CC – Ortak Kriterler), ortak ihtiyaçlar için ortak ifadeler kaynağı sunmaktadır ve ortak bir değerlendirme metodunu desteklemektedir. CC "koruma profilleri" ve "güvenlik hedefleri" kullanımı, Bilişim Teknolojileri işlevlerine sahip olan ürünlerin (ve bir dereceye kadar sistemlerin) geliştirilmesine önemli derecede yardımcı olmaktadır. CC metodunun tekrar edilebilirliği ve titizlikle hazırlanmış olması, kullanıcı güvenlik ihtiyaçlarının kapsamlı bir şekilde tanımlanmasını sağlamaktadır. Güvenlik hedefleri, sistem entegratörlerine bileşiklerin tedarikinde ve güvenli Bilişim Teknolojileri sistemlerinin uygulanmasında gerekli olan anahtar bilgiyi sunmaktadır.

14. Güvenliği, güvenli ve makul teknoloji geliştirme süreçleri de dahil olmak üzere yeni teknolojilerin düzenli olarak edinilmesine imkan sağlayacak şekilde tasarlayın.

Görev ve işlem süreçleri ile tehdit çevreleri değiştikçe güvenlik gereklilikleri ve teknik koruma metotları da güncellenmelidir. Görev ve işlemlere yönelik Bilişim Teknolojileri ile ilgili riskler zamanla çeşitlenmekte ve periyodik değerlendirmeden geçmektedir. Periyodik değerlendirme, sistem tasarımcılarının ve yöneticilerinin güvenlik yeterliliğine yönelik değişiklik ya da güncellemeler ile tanımlanmış riskleri kabul edip etmeyeceği ya da etkiyi azaltıp azaltmayacağı konusunda bilinçli risk yönetimi kararları almasını sağlayacak şekilde uygulanmalıdır. Tutarlı güvenlik çözümü, yeniden değerlendirme ve gelişen, uygulanabilir BT zaaflarının zamanında tanımlanmaması sahte bir güven ortamı ve artan risk ile sonuçlanacaktır.

Her bir güvenlik mekanizması, bütün bir sistemin tekrar tasarlanmasını gerektirmeden yeni teknolojiye geçişi ve yeni özelliklerin güncellenmesini destekleyebilecek durumda olmalıdır. Güvenlik tasarımı, bütün sistemin değiştirilmesi gerekmeden tüm bağımsız parçaların güncellenebilmesini sağlamak için modüler bir yapıda olmalıdır.

15. İşlemsel kullanım kolaylığı için çaba harcayın.

Bir güvenlik kontrolünü sürdürmek ve işlemek ne kadar zorsa, kontrolün daha az etkili olması o kadar muhtemeldir. Bu nedenle, güvenlik kontrolleri işlemler kapsamı ve önemli bir faktör olarak kullanım kolaylığı ile tutarlı olacak şekilde tasarlanmalıdır. Yöneticiler ve kullanıcıların tecrübesi ve uzmanlığı, güvenlik kontrolünün işlenmesine uygun ve orantılı olmalıdır. Kuruluş, sistem yöneticilerinin ve kullanıcılarının düzenli olarak eğitildiğinden emin olmak için gerekli kaynaklara yatırım yapmalıdır. Dahası, döngü işlemsel maliyetlerle birlikte yönetici ve kullanıcı eğitim maliyetleri, güvenlik kontrolünün maliyet verimliliğini karar verirken göz önünde bulundurulmalıdır.

DAYANIKLILIĞI ARTTIRIN

16. Katmanlı güvenlik uygulayın (tek bir zaaf bile olmadığından emin olun).

Güvenlik tasarımları, belirli bir tehdidi belirlemek ya da ondan korunmak ya da zafiyeti azaltmak için katmanlı bir yaklaşımı ele almalıdır. Örneğin, bir saldırganın başarılı bir şekilde sisteme saldırması için kullanması gereken iş faktörünü arttırmak için uygulama geçidi ve izinsiz giriş tespit sistemi ile birlikte bir filtreleme yönlendiricisi kullanımı. Sistemin güvenlik duruşunu daha da geliştirmek için sağlam şifre kontrolleri ve yeterli düzeyde kullanıcı eğitimleri ekleyin.

Çoklu, örtüşen koruma yaklaşımları kullanıldığında herhangi bir bağımsız koruma yaklaşımı arızası ya da sahtekarlığı durumunda sistem korunmasız kalmayacaktır. Kullanıcı eğitimleri ve farkındalığı, iyi yapılandırılmış politika ve süreçler ile koruma mekanizmalarının fazlalığı aracılığıyla katmanlı korumalar görev hedeflerini gerçekleştirme amacıyla bilgi teknolojilerinin etkili korunmasını sağlar.

Katmanlı koruma ihtiyacı, özellikle COTS ürünler kullanıldığında önemlidir. Pratiğe dayalı tecrübeler gösteriyor ki COTS ürünlerdeki en gelişmiş güvenlik kalitesi, karmaşık saldırılara karşı yüksek derecede bir koruma sağlamamaktadır. Kontrolleri seri halde yerleştirerek –ki bu saldırganların hedeflerine ulaşmak için daha fazla çaba harcamasını gerektirir- mevcut durumun etkilerini azaltmak mümkündür.

17. Zararı sınırlandırmak ve dayanıklılık gösterebilmek için bir Bilişim Teknolojileri sistemi tasarlayın ve işletin.

Bilgi sistemleri saldırılara karşı dirençli olmalı, zararı sınırlandırabilmeli ve saldırı gerçekleştiğinde hızlıca bundan kurtulabilmelidir. Burada önerilen ilke, herhangi bir olası siber saldırıya etkili bir şekilde karşılık verileceğini garanti etmek için tüm katmanlarda yeterli sayıda koruma teknolojileri bulunması ihtiyacını göstermektedir. Onarılamayan, henüz onarılmamış, bilinmeyen ve onarılabilen fakat artan işlemsel yeterliklere izin vermek için onarılmamış (güvenlik duvarından geçişine izin verilmiş riskli hizmetler gibi) zafiyetler bulunmaktadır. Güvenli bir başlangıç durumu sağlamaya ek olarak, güvenli sistemler ister güvenli bir aksama durumu ister bilinen güvenli bir duruma karşı bir kurtarma süreci aracılığıyla aksamadan sonra da iyi tanımlanmış bir pozisyonda olmalıdır. Kuruluşlar yeterlikleri kurmalı, tespit etmeli ve karşılık vermelidir; sistemlerindeki aksamanın her noktasını yönetmeli ve bir bildirme-müdahale etme stratejisi uygulamalıdır. (14. İlke ile ilgilidir.)

18. Sistemin beklenen tehditler karşısında dirençli olduğunun ve öyle olmaya devam edeceğinin güvencesini sağlayın.

Güvence, bir sistemin güvenlik beklentilerini karşıladığına dair güven gerekçesidir. Bu beklentiler, hem direkt sızmalara hem de güvenlik kontrollerini bozmaya yönelik girişimlere karşı yeterli direnci sağlama olarak özetlenebilir. Tehdit ortamının, gerekliliklerin değerlendirilmesinin, donanım ve yazılım mühendisliği disiplinlerinin ve ürün ve sistem değerlendirmelerinin iyice anlaşılması güvenceyi sağlamak için kullanılan ana kriterlerdir. Ek olarak belirli ve gelişen tehditlerin dokümantasyonu, uygulamalı güvenlik alanında zamanında düzenlemeler yapmada ve artan güvenlik iyileştirmelerini stratejik olarak desteklemede önemli bir konuma sahiptir.

19. Zafiyetleri sınırlayın ya da kontrol altına alın.

Zafiyetleri sınırlamak ya da kontrol altına almak üzere sistemleri tasarlayın. Bir zafiyet ortaya çıktığında zarar sınırlandırılmış ya da kontrol altına alınmış olabilir; bu da diğer bilgi sistemi ögelerinin düzgün bir şekilde işlemesine izin verecektir. Güvensizlikleri sınırlamak ve kontrol altına almak aynı zamanda ihtiyaç anında en çok bilgi sistemi alanlarına yönelik olarak müdahale ve tekrar yapılandırma çabalarına odaklanılmasına yardımcı olacaktır. (10. İlke ile ilgilidir.)

20. Kamuya açık sistemleri, kritik görev kaynaklarından ayırın (veri, süreçler vb.).

Birçok durumda paylaşımlı altyapıya karşı eğilim kayda değer olsa da bu, evrensel olarak uygulanabilir değildir. Bilginin hassasiyeti ve kritik olma durumun yüksek olduğu durumlarda kuruluşlar, verinin depolandığı sistem sayısını sınırlandırmak ve onları fiziksel ya da mantıksal çerçevede ayrıştırmak isteyebilirler. Fiziksel ayrıştırma, kuruluşun kamuya açık bilgi kaynakları ile kritik bilgileri arasında hiçbir fiziksel bağlantı bulunmadığını garanti etmeyi içerebilir. Mantıksal ayrıştırma çözümleri uygulanırken, güvenlik hizmetleri ve mekanizmalarının katmanları, kamuya açık sistemler ve kritik görev kaynaklarını korumakla sorumlu güvenli sistemler arasında kurulmalıdır. Güvenlik katmanları, arındırılmış bölge ve perdelenmiş alt ağlar gibi ağ mimarisi tasarımlarını içerebilir. Nihayetinde sistem tasarımcıları ve yöneticileri, kamuya açık sistemlerin kullanımına ilişkin kurumsal güvenlik politikaları ve süreçlerini yürütmelidir.

21. Programlama sistemleri ve ağ altyapılarını ayırmak için sınır mekanizmalarını kullanın.

Programlama ve iletişim altyapılarında ağ sınırları boyunca bilgi ve bağlantı akışını kontrol etmek ve kullanıcı gruplarının düzgün bir şekilde ayrımını hızlandırmak için birtakım bağlantı kontrol aygıtları ve eşlik eden bağlantı kontrol politikaları kullanılmalıdır. Ağ sınırları boyunca iletişim için aşağıda sıralananlar hakkında karar vermek gerekir:

- Hangi harici arabirimlerin gerektiği,
- Bilginin “push”[1] mu “pull”[2] mu olduğu,
- Hangi portların, protokollerin ve ağ hizmetlerinin gerektiği,
- Sistem bilgi değişimleri için hangi gerekliliklerin olduğu; örneğin, güven ilişkileri, veri tabanı replikasyon hizmetleri ve alan adı çözümleme süreçleri gibi.

22. Yetkisiz kullanımları saptamak ve olay araştırmalarını desteklemek için denetim mekanizmaları tasarlayın ve uygulayın.

Kuruluşlar, yetkisiz kullanımları saptamak ve sistem kaynaklarının düzgün bir şekilde işlediğinden emin olmak için denetim günlüklerini izlemeli, kaydetmeli ve periyodik olarak incelemelidir. Bazı durumlarda kuruluşların, denetleme mekanizmalarından elde edilen bilgiyi uygun durumundaki üçüncü taraflar, emniyet yetkilileri ya da Bilgi Edinme Özgürlüğü Kanunu (FOIA) ‘na başvuranlar ile paylaşması gerekebilir. Çoğu kuruluş, ‘yetkisiz kullanım kanıtlarının (denetim geçmişi gibi) idari ya da cezai soruşturmaları desteklemek için kullanılabileceği’ ifadesini içeren politikaların izlenmesi için onay vermektedir.

23. Gerekli ulaşılabilirliği sağlamak için beklenmedik olay ve felaket durumunda kurtarma prosedürleri geliştirin ve uygulayın.

İşlemlerin, planların ve felaket atlatma prosedürlerin sürekliliği, bir şirketin bir felaket ya da uzun süreli hizmet kesintileri gibi kuruluşun işleyişini etkileyen durumlarda kuruluş işlemlerinin devamlılığı anlamına gelmektedir. Bu tarz planlar bir acil müdahale aşaması, bir kurtarma aşaması ve normal işletime dönüş aşamasından oluşmaktadır. Bir olay olması durumunda çalışan sorumlulukları ve ulaşılabilir kaynaklar belirlenmelidir. Gerçekte arıza ve felaket kurtarma planları her olası senaryo ya da varsayımı içermemektedir. Bunun yerine gerçekleşmesi en muhtemel olaylara odaklanır ve kabul edilebilir bir kurtarma metodunu işaret eder. Tüm plan ve prosedürler, etkili olduklarından ve iyice anlaşıldıklarından emin olmak için periyodik olarak uygulanmalıdır.

ZAFİYETLERİ AZALTIN

24. Basitliği sağlamaya çalışın.

Mekanizma ne kadar karmaşıksa, kötüye kullanılabilecek çatlaklara sahip olma oranı o derecede artacaktır. Basit mekanizmalar, daha az çatlağa sahiptir ve daha az bakım gerektirir. Dahası, konfigürasyon yönetimi işlemleri basitleştirilmiş olduğundan basit bir mekanizmayı güncellemek ya da değiştirmek daha az yoğun bir süreç olacaktır.

25. Güvenilecek sistem ögelerini en aza indirin.

Güvenlik önlemleri insanları, işlemleri ve teknolojiyi kapsamaktadır. Teknolojinin kullanıldığı yerlerde korumayı sürdürmek için minimum sayıdaki sistem ögesine güvenilmesi gerekecek şekilde donanım, aygıt yazılımları ve yazılımlar tasarlanmalı ve uygulanmalıdır. Dahası, sistem güvenlik özelliklerinin uygun maliyetli ve zamanında sertifikasyonunu sağlamak amacıyla sistem için en güvenli işlevleri sunması beklenen yazılım ve donanım miktarını en aza indirmek önem taşımaktadır.

26. Ayrıcalıkları en aza indirin.

Erişimi sınırlandırma ya da “minimum ayrıcalık” kavramı, basitçe gerekli işlevleri yürütmek için gerekli olandan daha fazla yetkilendirme sağlamamak anlamına gelmektedir. Bu, belki de en çok sistemin idaresinde uygulanmaktadır. Amacı, kritik sistem güvenlik kontrollerine erişimi olan kişi sayısını sınırlandırarak riski azaltmaktır (sistem güvenlik özelliklerini aktif ya da etkisiz hale getirme ya da kullanıcılara ya da programlara tanınan ayrıcalıkları değiştirebilme yetkisini sahip olanları kontrol etme gibi). En iyi uygulama, “üstün kullanıcı” vasıflarına sahip olan bir kişi yerine güvenlik kaynaklarına sınırlı erişim yetkisi olan birden çok yöneticiye sahip olmanın daha iyi bir seçenek olduğunu göstermektedir.

Dikkatler yalnızca idari değil sistem kullanımının çeşitli türleri için de rol-odaklı erişim kontrollerini uygulamaya verilmelidir. Sistem güvenlik politikası, kullanıcılar ve işlemler için çeşitli rolleri saptayıp tanımlayabilir. Her bir rol, işlevlerini yerine getirmek için gereken izinlere göre tahsis edilir. Her bir izin, belli bir kaynağa izinli bir erişimi belirtir (belli bir dosya ya da rehberi “okuma” ve “yazma” erişimi, sunulan “host” ve “port”a “bağlanma” erişimi gibi). İzinler açık bir şekilde onaylanmadığı sürece kullanıcı ya da

süreç korunan kaynağa erişememelidir. Bunun dışında, güvenlik amaçları doğrultusunda ayrı kalması gereken rol ve sorumlulukları belirlemeniz gerekmektedir (bu durum genellikler "görevler ayrılığı" olarak isimlendirilir).

27. Gereksiz güvenlik mekanizmaları uygulamayın.

Her güvenlik mekanizması bir güvenlik hizmetini ya da hizmetler serisini desteklemelidir ve her güvenlik hizmeti de bir ya da daha fazla amaca sahip olmalıdır. Eğer yetkili bir hizmeti ya da güvenlik hedefini desteklemiyorlarsa ekstra önlemler uygulanmamalıdır. Böylesi mekanizmalar sisteme ihtiyaç duyulmayan bir karmaşıklık getirebilir ve fazladan oluşabilecek zafiyetlerin olası kaynaklarıdır.

Yetkisiz dosya erişimlerini önleyerek güvenilirlik ve bütünlük hedeflerini destekleyen kontrol hizmetine erişimi kontrol eden dosya şifreleme durumu örnek olarak verilebilir. Eğer dosya şifreleme, hedefleri yerine getirmek için gerekli bir adımsa o zaman bu mekanizma uygundur. Ancak bu güvenlik hedefleri dosya şifreleme olmadan da yeterince destekleniyorsa o zaman bu uygulama gereksiz bir sistem karmaşası haline gelecektir.

28. Sistemin kapanması ya da tasnifi durumunda devamlı güvenlik sağlayın.

Bir sistemin gücünün kesilmesi ve kapanması durumunda kritik bilgiler hala sistemde yer alır ve yetkisiz bir kullanıcı ya da kuruluş tarafından elde edilebilirler. Kritik bilgi sistemlerine erişim her zaman kontrol edilmelidir.

Bir sistemin kullanım süresinin sonunda sistem tasarımcıları bilgi sistemi varlıklarını düzgün ve güvenli bir şekilde devretmek için süreçler geliştirmelidir. Bu süreçler, sistem hard diskleri, geçici bellek ve diğer medyaların kabul edilebilir bir seviyeye kadar tasfiye edildiğinden ve artık bir bilgi içermediğinden emin olmak için uygulanmalıdır.

29. Yaygın hata ve zafiyetleri saptayın ve önleyin.

Çoğu hata rahatsız edici bir düzenlilikte tekrar meydana gelir – örneğin; arabellek aşımı, hız durumu, format hataları, girdi geçerliğini kontrol edememe ve aşırı derece imtiyaz tanınan programlar gibi. Geçmişten ders çıkarmak gelecekte alacağınız sonuçlara fayda sağlayacaktır.

AĞ İLE İLGİLİ PLANLAMALAR YAPIN

30. Fiziksel ve mantıksal olarak dağıtılan önlemler serisi aracılığıyla güvenliği uygulayın.

Genellikle tek bir güvenlik hizmeti ayrı makinelerde bulunan ögelerin işbirliği ile sağlanır. Örneğin, sistem yetkilendirmesi; ağ ögeleri yardımıyla çalışma alanındaki kullanıcı arayüzünden yetkilendirme sunucusu üzerindeki bir uygulamaya kadar uzanan ögeleri kullanarak elde edilir. Sağlanan güvenlik hizmeti ile tüm ögeleri ilişkilendirmek önemli bir detaydır. Altyapı kaynakları daha üst düzey bütçe ve işlemsel kontrol altında olduğundan güvenliği sağlamak için bu bileşenlerin sistem boyunca paylaşılması daha mümkündür.

31. Çoklu örtüşen bilgi alanlarına yönelik güvenlik önlemleri şekillendirin.

Bilgi alanı, aktif işletmeler ve bunların veri nesneleri serisidir. Tek bir bilgi alanı çoklu güvenlik politikalarına tabi olabilir. Tek bir politika, çoklu bilgi alanlarını kapsayabilir. Etkili ve uygun maliyetli

güvenlik yeterliği, bilgiyi ve veriyi işleyen ilgili bilgi sistemlerini fiziksel olarak ayırma ihtiyacı duymadan çoklu bilgi alanlarını korumak için çoklu güvenlik politikalarını icra edebilmelidir. Bu ilke, çeşitli hassasiyet seviyeleri için ayrı LANlar ve altyapılar oluşturmaya dayanan geleneksel uygulamadan (güvenlik sınıflandırması ya da teklif geliştirme gibi işletme işlevleri) uzaklaşıp ortak, paylaşılan, işletim sisteminde uygun korumalara sahip altyapılar, uygulama ve çalışma yeri seviyesi kullanımına olanak sağlayan çözümlere yönelmeyi savunmaktadır.

Bunlara ek olarak, görevleri gerçekleştirmek ve kritik işlevleri korumak için kuruluşların himaye etmesi gereken birçok bilgi türü bulunmaktadır. Bu ilke göz önünde bulundurulduğunda sistem mühendisleri, mimarlar ve Bilişim Teknolojileri uzmanları çoklu bilgi hassasiyeti seviyelerine sahip kuruluşların etkili bir şekilde temel güvenlik hedeflerini gerçekleştirmesini sağlayacak bir güvenlik yeterliği geliştirmelidir.

32. Alanlar içinde ve alanlar boyunca gerekli erişim kontrol kararlarının verildiğinden emin olmak amacıyla kullanıcı ve süreçler için yetkilendirme yapın.

Yetkilendirme, bir sistemin istenen eylemi uygulamak üzere bir bireyin, sürecin ya da makinenin uygun olma durumunu saptadığı ya da bir iletimin ve mesajın geçerliğini oluşturduğu süreçtir ve böylece güvenliğin güvenilmeyen bir kaynak tarafından riske atılmadığından emin olmamızı sağlar. Güvenlik politikalarını uygulamak ve güvenlik hedeflerini gerçekleştirmek için yeterli yetkilendirmenin yapılmış olması zorunludur.

Bunlara ek olarak, alanlar arası etkileşimlerde güven seviyesi her zaman önemli bir meseledir. Çözüm, bir yetkilendirme politikası kurmak ve bunu gerekli olduğunda alanlar arası etkileşimlere uygulamaktır.

Not: Bir kullanıcının çoklu alanlarda birden fazla isim kullanma hakkı olabilir. Dahası, haklar alanlar boyunca farklılık gösterir ve bu da güvenlik politikası ihlallerine yol açabilir.

33. Yükümlülüğü sağlayabilmek için tek (eşsiz) kimlikler kullanın.

Kimlik, gerçek bir kullanıcıyı ya da kendi kimliğine sahip bir süreci (uzaktan erişim sağlayan bir program gibi) temsil edebilir. Aşağıdakileri yerine getirebilmek için eşsiz kimlik kullanımı gerekli bir öge olmalıdır:

- Bir kullanıcının ya da sürecin hesap verme zorunluluğunu ve izlenebilirliğini sürdürme
- Bir bireysel kullanıcı ya da sürece özel haklar verme
- Erişim kontrol kararlarını güçlendirme
- Güvenli haberleşme yollarında emsallerin kimliklerini oluşturma
- Yetkisiz kullanıcıların yetkili bir kullanıcıymış gibi davranmasını önleme

5. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.