1. Amaç

Bu politikanın amacı kurum kaynaklarına ilişkin yapılacak sızma testleri(pentest) standartlarını belirlemektir. Bu politika, kurumun bilgi güvenliğinin sağlanmasına yardımcı olmak için tasarlanmıştır.

2. Kapsam

İşbu politika 'KTÜN'e ait olan' veya 'KTÜN'e ait herhangi bir kablolu veya kablosuz iletişim ağına bağlı olan' bütün yazılımları/donanımları, KTÜN'ün kendi lokasyonlarında konuşlandırdığı veya hizmet aldığı firmalarda barındırdığı sistemleri, 'KTÜN kullanıcı hesapları' ile 'bu hesapların sahibi olan kişileri (sosyal mühendislik için) ; tüm bunlardan sorumlu 'kişileri'/'birim yöneticilerini'; tüm bunlar üzerinde 'pentest çalışması yapacak/yaptıracak' herkesi kapsamaktadır.

3. Dayanak:

3.1. 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanan "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" .

3.2. KTÜN TS ISO/IEC ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YÖNERGESİ

3.3. 06.07.2019 tarih ve 30823 sayılı Resmi Gazete'de Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi gereği Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberi.

3.4. Kişisel Verilerin Korunması Kanunu Teknik Tedbirleri.

3.5. 6085 sayılı Sayıştay Kanunu'nun Bilişim Sistemleri Denetimi kapsamındaki maddeleri ve Sayıştay tarafından onaylanarak yürürlüğe giren "Bilişim Sistemleri Denetimi Rehberi".

4. Tanımlar

4.1. PENTEST: Sızma(Penetrasyon) Testi. Sistemlerin saldırganların teknikleriyle test edilerek zafiyetlerin gösterilmesi.

4.2. YÜKLENİCİ: Pentest işini yapacak olan gerçek veya tüzel kişiler.

4.3. SOME: Siber Olaylara Müdahale Ekibi.

4.4. Güvenlik Denetimi: Mevcut güvenlik tedbirlerinin analiz edilmesi, politikaların etkinliğinin ve uyumluluğunun değerlendirilmesi.

4.5. Kurum: KTÜN (Konya Teknik Üniversitesi).

5. Sorumlular

Bu politikanın oluşturulmasından BİDB ve onaylamasından BGYS komisyonu sorumludur. Uygulanmasından, KTÜN Birim Yöneticileri ile KTÜN kaynaklarında pentest yapacak olan herkes(personel, öğrenciler, pentest hizmeti alınan tedarikçiler, iç-dış paydaşlar, dahili-harici siber güvenlik araştırmacıları vb.) sorumludur.

6. Hedefler

6.1. KTÜN Kaynaklarında PENTEST gerçekleştirecek olanların uyması gereken kuralları belirlemek.

6.2. KTÜN kaynaklarında hangi zamanlarda ve şartlarda PENTEST yapılacağını belirlemek. (Birim yöneticilerinin sorumlu olduğu alanlarda PENTEST işlemleri için neler yapması gerektiğini belirlemek.)

6.3. KTÜN kaynaklarında yapılacak PENTEST'ler için hazırlanan şartname veya sözleşme gibi anlaşma metinlerinin refere edeceği politika dökümanını oluşturmak. (Örneğin kullanacağı bir yazılım için PENTEST yaptırmak isteyen bir KTÜN birimi yüklenici ile yapacağı sözleşmede işbu POLİTİKA'ya refere ederek "YÜKLENİCİ KTÜN PENTEST POLİTİKASI 'Genel Kurallar' başlığı altında yazanlara uymakla mükelleftir" gibi bir ibare koyabilir.)

6.4. KTÜN'ün PENTEST çalışmalarından aşağıdaki kazanımları elde etmesini sağlamak:

6.4.1. Gerçek bir saldırganın kullandığı yöntemlerin ve bakış açısının kullanılması, bu sayede rutin kontrollerde tespit edilemeyen güvenlik zafiyetlerinin belirlenerek kapatılması.

6.4.2. Güvenlik açığı tespitlerinin, alınan güvenlik tedbirlerinin ve siber güvenliği ilgilendiren politikaların/prosedürlerin yeterli olup olmadığını ortaya çıkarmak.

6.4.3. Ulusal güvenliği ilgilendirebilecek hassas veriler, kişisel veriler ve kritik kurumsal verilerde yüksek riskli hedeflerin belirlenmesini, korunmasını, risk yönetimini ve sektördeki mevcut güvenlik standartlarıyla uyumluluğu sağlamak,

6.4.4. Hangi düşük riskli güvenlik açıklarının sömürülmesinin yüksek seviyelerde çok fazla hasara yol açabileceğini tespit etmek.

6.4.5. Siber güvenlik farkındalık eğitimi ihtiyacını belirlemek.

6.4.6. Teknolojiye ve personele gereken maddi ya da eğitimsel yatırım ile ilave personel ihtiyaçlarını belirlemek.

7. KTÜN Pentest Uygulamaları ve Periyotları

7.1. KTÜN SOME ekibi, işbu politikanın "**SOME Pentestleri**" başlığı altında geçen periyotlarda ve şartlarda pentestler yapacaktır.

7.2. Kurum, ihtiyaç görmesi halinde **zaman zaman kurum dışından da pentest hizmeti** alarak kurum çalışanı olmayan uzmanlar gözüyle de testlerin yapılmasını sağlayabilecektir.

7.3. Zaman zaman kurum dışından alınan pentest hizmetlerinde kısmi alanlarda testler yaptırılabilir fakat işbu politikanın "**Tam Kapsamlı Pentest**" başlığı altında geçen periyotlarda ve şartlarda pentestler mutlaka yaptırılacaktır.

7.4. Kurum, işbu politikada yer alan şartlara riayet etmek şartıyla zaman zaman zafiyetlerin belirlenmesine yönelik çalışmalar(bugbounting, vdp, ctf, öğrenci projeleri vb.)

düzenleyebilecektir.

7.5. Aşağıdaki durumlarda en kısa sürede ilgili sistemler üzerinde zafiyet taraması çalışması yapılacaktır(Birim yöneticileri aşağıdaki durumlarda KTÜN SOME ekibine bilgi vermelidir):

7.5.1. Birimin yeni bir lokasyona taşınması, yeni bir ağ altyapısının devreye alınması veya mevcut olanı önemli ölçüde değiştirme gibi altyapı değişikliği durumlarında,

7.5.2. Yeni bir yazılımın veya donanımın devreye alınması ya da mevcut olan sistemde büyük değişiklikler yapılması durumunda,

7.5.3. Daha önceden bildirilen bir zafiyetin giderildiğine dair geri dönüş geldikten sonra kritiklik derecesine göre gerçekten giderilip giderilmediğinin denetlenmesi durumunda,

7.5.4. Herhangi bir sistemde sistemin zafiyetleri ile ilişkili olma ihtimali olan bir siber olay meydana geldiğinde,

7.5.5. Güvenlik politikalarında zafiyet bulma çalışması yapılmasını gerektiren değişiklikler olması durumunda,

7.5.6. Kurum birimlerinin (ağ, sistem, yazılım geliştirme vb.) talepleri olduğunda,.

8. Genel Kurallar

8.1. Pentestlerde Kapsam

8.1.1. Sızma testlerinde kapsam net olarak belirtilerek dokümante edilmeli ve sızma testi yapanlar tanımlanan kapsama uymalıdır.

8.1.2. Pentest işlemi kapsam dahilindeki tüm unusurlar için tüm zafiyet taramalarını içermelidir.

8.1.3. **Sızma Testi Gerçekleştirilemeyen Bileşenlerin Yönetimi:**

Operasyonel ortamda olup sızma testi yapılması mümkün olmayan veya yüksek risk içeren sistemler için "bu sistemlerde bulunan kritk verilerin anonimleştirilmiş hallerinin olduğu kopya sistemler(gerçeğine benzer test ortamları) oluşturularak" yapılacak pentestler bu kopya sistemler üzerinde yapılmalıdır. (Test ortamının oluşturulması mümkün olmayan her bir bileşen için güvenlik denetimi ve sıkılaştırma işlemleri uygulanmalıdır.)

8.2. YÜKLENİCİ ile KTÜN Arasındaki İletişim:

8.2.1. YÜKLENİCİ ile KTÜN arasındaki tüm iletişim, koordinasyon, ve yazışmalar belirli kişiler arasında yapılacak olup bu kişilerin iletişim bilgileri sözleşmenin imzalanması sonrası ilgili taraflarca birbirlerine iletilecektir (Bu iletilen bilgiler içinde Acil Duruma geçilmesi safhasında iletişime geçilecek kişi ve yönetici iletişim bilgileri de mutlaka olmalıdır).

8.2.2. Sızma testleri esnasında, KTÜN gerçek siber saldırılara da maruz kalabileceğinden KTÜN, sızma testlerini izleyerek, testler ile siber saldırılar arasında ayrım yapabilmeli ve YÜKLENİCİ

ile iletişim kurarak, testi durdurmasını sağlayabilmelidir. (Testin siber saldırı esnasında durdurulması, hem sistemi korumak açısından hem de sonradan yapılacak olan adli bilişim analiz çalışmasını da kolaylaştırması açısından önemlidir.)

8.3. KTÜN'ün YÜKLENİCİ'ye karşı Feragatnamesi

8.3.1. YÜKLENİCİ tarafından KTÜN'e verilecek hizmetin ön hazırlıkları sırasında, saldırı testleri öncesi ve saldırı testleri sırasında eğer varsa tüzel ve/veya gerçek üçüncü kişileri, haberdar etmek, gerekiyorsa onlardan yazılı ve/veya sözlü olarak gerekli her türlü izni almak ve testler sırasında gözlemlerini yaptırmaktan KTÜN sorumludur. Bilgi verilmemiş, izin alınmamış veya gözlem yaptırılmamış tüzel ve/veya gerçek üçüncü kişilerle çıkacak anlaşmazlıklardan, bu üçüncü kişilerin taleplerinden ve bu sebeple doğabilecek doğrudan ve/veya dolaylı zararlardan dolayı YÜKLENİCİ'nin sorumlu olmadığını KTÜN kabul eder. KTÜN YÜKLENİCİ'yi bu anlaşmazlıklardan, taleplerden ve zararlardan ari tutacaktır.

8.3.2. YÜKLENİCİ'nin ağır kusuru ile sebep olduğu haller hariç olmak üzere, saldırı testleri sırasında KTÜN'nün DoS, DDoS veya test sistemlerinin zarar görmesi ve bunun hizmet kesintisine veya sistem yüklenmelerine sebep olması halinde YÜKLENİCİ'nin sorumlu olmayacağını KTÜN kabul eder.

8.4. Gizlilik

8.4.1. Bulunan zafiyetler sadece SOME ekibi ile paylaşılacak olup kurum çalışanı olsun olmasın başkalarına iletilmeyecektir. KTÜN onaylı Online platformlardan (bugbounting, VDP vb.) yapılan bildirimler SOME ekibine yapılmış sayılacaktır.

8.4.2. YÜKLENİCİ, gerçekleştirdiği bu hizmete dair KTÜN'ün yazılı izni olmadan kurumsal ismini, logosunu yazılı ya da sözlü hiçbir şekilde kullanmayacak veya referans olarak yayımlamayacaktır.

8.4.3. Sızma testleri gerçekleştirilmeden önce testi gerçekleştirecek taraftan, test süresince elde edilen hiçbir verinin yetkisiz kişilere verilmemesi, aktarılmaması ve ifşa edilmemesine yönelik taahhüt alınacaktır. Verilecek taahhütler, KTÜN tarafından açılan zafiyet bulma programları(bugbounty, VDP vb.) online platformları üzerinden verilen taahhütler şeklinde de olabilir.

8.4.4. Sızma testi ile ilgili gerek kurum tarafından doldurulan anket, form vb. dokümanlar gerekse YÜKLENİCİ tarafından üretilen sızma testi sonuç raporu vb. dokümanlar gizlilik derecesine haiz dokümanlardır. Bu tür dokümanlar üretim, kullanım ve saklama aşamalarında hassasiyetle ele alınmalı ve çalınma, yetkisiz erişim, kaybolma vb. risklere karşı korunmalıdır.

8.4.5. Test raporlarına erişim, bilmesi gereken prensibine göre verilmeli, yetkilendirilmeli ve kontrol edilmelidir. Raporlara erişim sadece testi yapan veya doğrudan yöneten kişiler ile kısıtlı kalmalı ve bunlar haricinde erişim olmamalıdır.

8.4.6. YÜKLENİCİ yaptığı testler esnasında KTÜN kullanıcılarının kişisel bilgilerine ulaşması durumunda, bu bilgileri personeli olduğu işyeri dahil kimse ile paylaşmamalı, sızma testi sonuç raporuna eklememeli ve kopyasını almamalı ve çalışmasını tamamladığında geri dönülemez

şekilde imha etmelidir. Sızma test raporunda kullanıcı adı ve parolaları maskelenmelidir.

8.4.7. Tüm kritik bilgiler(zafiyetler, raporlar vb.) şifrelenerek iletilecektir. (Şifrelemede PGP gibi asimetrik şifreleme tekniklerine öncelik verilecektir.)

8.4.8. Penetrasyon Testi ve Doğrulama Testi ile ilgili raporlama ve tüm kayıtlar, YÜKLENİCİ tarafından, test hizmeti süresi sonunda, KTÜN'e teslimini müteakip geri döndürülemez şekilde yok edilecek, herhangi bir kopyası tutulmayacak ve KTÜN'e bu işlemin tamamlandığına dair bildirimde bulunacaktır.

8.4.9. YÜKLENİCİ test ekibindeki kişiler, KTÜN web sitesinde yayımlanan **"ÜÇÜNCÜ TARAF BİLGİ GÜVENLİĞİ GİZLİLİK SÖZLEŞMESİ"** ile **"KTÜN Kurum Dışı Gerçek veya Tüzel Kişilerle Yapılacak Kişisel Verilerin Korunması Sözleşmesi"ni** okuyup anlayarak hükümlerine uyacaktır.

8.5. Hizmetlerin Sürekliliği

8.5.1. Testler sırasında KTÜN hizmetlerinin kesintiye uğramaması sağlanmalıdır. KTÜN sistemlerinde hizmet kesintisine ya da zarara neden olabilecek test türleri için KTÜN'e özellikle bildirimde bulunulacak ve onay alınacaktır. Bu tür testlerin zamanlaması planlanırken aşağıdaki gibi hususlarla çakışmamasına özen gösterilecektir:

- Öğrenci/ders kayıtları, kritik online etkinlikler (sınav/toplantı/eğitim/webinar vb.),

- BT Sistemleri Güncelleme/Bakım/Onarım Çalışmaları,

8.5.2. Sızma testleri için mümkün olduğu kadar test edilecek sistemde yoğunluk olmayan saatlerin seçilmesine özen gösterilecektir. Gün içinde çalışması kritik olan sistem ve yazılımlar için mesai saatleri dışında bir zaman dilimi seçilecektir. DoS/DDoS saldırı testi düzenlenecek ise, mesai saatleri dışı seçilecektir.

8.5.3. Hizmet kesintisine neden olabilecek testler esnasında sistemin işleyişi KTÜN sorumluları tarafından izlenecek ve sistemde bir sorun tespit edildiği takdirde, test sorumlusuna konuyla ilgili bilgi verilerek testlere ara verilmesi sağlanacaktır. Sistemde tespit edilen sorun uzun süreli veya önemli ise testler daha sonraki bir tarihe ertelenebilecektir.

8.6. Sızma Testi için Kullanılan Hesapların Yönetimi:

8.6.1. Sağlıklı ve gerçek hayata uygun bir sızma testi için testler sırasında farklı yetki seviyesindeki kullanıcı profilleri(anonim kullanıcılar, misafir kullanıcılar, çalışanlar, kurumdan hizmet alan kullanıcılar ve kuruma destek veren kullanıcılar, adminler vb.) kullanılmalıdır, KTÜN bunun için SOME Ekibi ilgili çalışanlarına gerekli kullanıcı hesaplarını verecektir. SOME ekibinde olmayanlardan (Kurum çalışanı/öğrencisi veya kurum dışı pentestçilerine) ise uygun gördüğü kişilere "KTÜN tarafından kritik olarak değerlendirilmeyen" sistemlere ait kullanıcı hesaplarını verebilecektir.

8.6.2. SOME ekibi dışındakilerin yapacağı "KTÜN tarafından kritik olarak değerlendirilen sistemlerin testleri" bizzat KTÜN SOME personeli ile birlikte KTÜN tarafından onaylanan yerde KTÜN'e ait cihazlar kullanılarak yapılacak olup bu kritik sistemlere ait kullanıcı hesap bilgileri kurum dışına çıkarılmayacaktır.

8.6.3. Sızma testini gerçekleştirmek için kullanılan herhangi bir kullanıcı veya sistem hesabı, yalnızca meşru amaçlar için kullanıldığından emin olmak için kontrol edilmeli, izlenmeli, kayıt altına alınmalı ve test bittikten sonra pasif hale getirilmelidir.

8.7. **Doğrulama Testlerinin Yaptırılması:**

Kapatılan güvenlik açıklarına yönelik doğrulama testleri görevlerin ayrılığı ilkesi doğrultusunda yapılmalıdır. (Doğrulama testini yapacak olan ile açıklığı kapatan farklı ekiplerdeki kişiler olmalıdır)

8.8. **Sızma Testi Sonuçlarının Raporlanması:**

8.8.1. Sızma testi bulguları karşılaştırılabilir bir puanlama yöntemi dikkate alınarak raporlanmalıdır.

8.8.2. Raporda aşağıdakiler detaylı şekilde belirtilmelidir:

8.8.2.1. Her bir test adımında uygulanan yöntemler ve kullanılan araçlar,

8.8.2.2. İncelenen sistemlere ilişkin tespit edilen işletim sistemi/çalışan servis ve sürümleri gibi bilgiler

8.8.2.3. Tespit edilen güvenlik zafiyetleri ekran çıktıları ve/veya video görüntüleri

8.8.2.4. Zafiyetlerin sebep olabileceği zararlar/sonuçları ve zafiyete ilişkin referans bilgileri

8.8.2.5. Zafiyetlerin sebep olabileceklerine ilişkin senaryolardan mümkün olanlar test edilerek ekran çıktıları ve/veya video görüntüleri

8.8.2.6. Başarılı olan sisteme sızma girişimleri

8.8.2.7. Zafiyetleri gidermek için yapılması gereken işlemlerin detaylı ve anlaşılır bir şekilde tarifi

8.8.2.8. Olası zafiyetlerin tekrarlanmaması için genel tasarım ve altyapısal iyileştirmelere de tavsiye niteliğinde yer verecektir

8.8.2.9. Test sırasında toplanan ayrıntılı loglar, veriler ve varsa sömürü kodlarının örnekleri

9. Tam Kapsamlı Pentest

9.1. Zaman zaman kurum dışından alınan pentest hizmetlerinde kısmi alanlarda testler yaptırılabilir fakat en fazla 3 yılda bir, kurum dışından hizmet alınarak aşağıdaki "**Tam Kapsam Unsurları**"nı da içeren tüm KTÜN kaynakları için kapsamlı bir pentest mutlaka yaptırılacaktır. "**Tam Kapsamlı Pentest**" tek seferde bir yükleniciye yaptırılacağı gibi, 3 yıllık bir periyot içinde aşama aşama 'bir veya birden fazla yükleniciye' de yaptırılabilir. (Örneğin bu yıl x,y,z sistemleri sonraki yıl m,n,t sistemleri gibi.)

9.2. YÜKLENİCİ, firma(tüzel kişi) olabileceği gibi şahıs(pentester gerçek kişisi) da olabilir. - Firmalar için TSE tarafından verilen "TS 13638/T2- Bilgi Teknolojileri- Güvenlik Teknikleri-

Sızma Testi Yapan Firma Belgesi" olmalıdır.

9.3. Yüklenicinin gerçek ya da tüzel kişi olmasından bağımsız olarak her halükarda aşağıdaki şartları taşıması gerekmektedir:

9.3.1. Test ekibinde yer alacak kişilerden en az birisinin aşağıdaki sertifikalardan en az ikisine sahip olması gerekmektedir:

- TSE Sızma Test Uzmanı Sertifikaları (Örneğin: TSE Kıdemli Sızma Test Uzmanı) .

- Uluslararası geçerliliği olan "Ethical Hacker, Red Team veya Penetration Tester" sertifikaları (Örneğin: LPT , CEH , OSCP, GPEN, eCPTx, eWPT, CRTP vb.) .

9.3.2. Sızma testi yapacak kişilerin Adli Sicil(Sabıka) Kaydı olmamalıdır.

9.4. **Tam Kapsam Unsurları:**

9.4.1. Aşağıdaki unsurların tümü test kapsamında olmalıdır:

9.4.1.1. KTÜN BT Sistemlerine dahil olan tüm bilişim kaynakları ve kullanıcıları,

9.4.1.2. KTÜN sistemlerinin olduğu tüm IP Blokları,

9.4.1.3. Hangi ağdan erişilebilir olduğundan (İnternetten ya da yerel ağdan ya da hiçbir ağa bağlı olmayan) bağımsız olarak tüm KTÜN cihazları.

9.4.1.4. Test kategorileri aşağıdakilerden KTÜN bünyesinde bulunanların tümünü içermelidir:
* Dış ve iç ağ sızma testi, tüm sistemlerde zafiyet taraması, zayıf parola testleri
* KTÜN tarafından geliştirilerek ya da dışarıdan hizmet alınarak kullanılan tüm yazılımlar, Web tabanlı hizmetler (web uygulamaları, API'ler, web servisleri vb.), Web tabanlı olmayan yazılımlar, mobil uygulamalar ve ödeme sistemleri
* Etki alanı , Sunucu, sanallaştırma sistemleri , son kullanıcı bilgisayarları, tablet-telefon gibi akıllı cihazların testleri, Veritabanı , E-posta , DNS , VPN ve proxy testleri
* Kamera, Turnike ve Geçiş sistemleri(Kartlı, tuşlamalı, biyometrik vb.) testleri
* Siber tehdit istihbaratı toplama çalışmaları ve Sosyal mühendislik testleri
* Kablolu veya Kablosuz ağ(wifi) ve ekipmanları, Network bileşenleri ve ikinci katman saldırı testleri, VoIP, Hizmet aksatma (DoS/DDoS), NAC/802.1x ve Fiziksel sızma testleri
* Güvenlik duvarı,"Saldırı tespit/engelleme", URL ve İçerik filtreleme testleri
* EKS(Endüstriyel Kontrol Sistemleri) / SCADA ve IoT sızma testleri

10. SOME Pentestleri

10.1. KTÜN SOME ekibi herhangi bir zaman dilimi ile sınırlı kalmaksızın tüm sistemler üzerinde sürekli bir şekilde pentest ve güvenlik denetimi çalışmaları yapmalıdır. Bu çalışmalar yılda en az 1 kez tüm sistemlerin üzerinden geçmiş olmalıdır.

11. Yaptırım

Bu politikanın ihlal edilmesi durumunda KTÜN BİLGİ GÜVENLİĞİ POLİTİKASI'nda belirtilen "POLİTİKANIN İHLALİ VE YAPTIRIMLAR" başlığı altındakiler geçerlidir.

12. Yürürlük

Bu politika, BGYS komisyonu tarafından onaylandıktan sonra Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

13. Yürütme

Bu politika, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.