KAYSERİ BÜYÜKŞEHİR BELEDİYESİ
SİBER VATAN YETKİNLİK MERKEZİ
YAZILIM TEKNİK ŞARTNAMESİ

İŞİN TANIMI : Kayseri Büyükşehir Belediyesi Sosyal Gelişmeyi Destekleme Programı (SOGEP) kapsamında yürütülen Siber Vatan Yetkinlik Merkezi Projesi için yazılım alımı işi.

İDARE : Kayseri Büyükşehir Belediyesi
İSTEKLİ : Teklif verecek olan gerçek veya tüzel kişi
YÜKLENİCİ : İşi yüklenecek olan gerçek veya tüzel kişi

1. SVYMEDUP Sanallaştırma Yazılımı (1 Adet)

1.1. Sanallaştırma yazılımı doğrudan fiziksel sunucu donanımı üzerine kurulan, performansı ve güvenliği artıran bir yazılım katmanı olmalıdır.

1.2. Sanallaştırma yazılımı istikrar ve performans sağlayan, tüm donanım kaynaklarını ve sanal makineleri yöneten mikro çekirdek yapısına sahip olmalıdır.

1.3. Sanallaştırma yazılımı fiziksel donanım kaynaklarını sanal kaynaklara dönüştürerek, sanal makinelerin donanım modelinden bağımsız çalışmasını sağlamalıdır.

1.4. Sanallaştırma yazılımı fiziksel sunucu üzerinde birden çok sanal makineyi izole edilmiş bir şekilde çalıştırarak donanım maliyetlerini düşürebilmelidir.

1.5. Sanallaştırma yazılımı hostların yönetimini (VM oluşturma, kaynak izleme) standart bir web tarayıcısı üzerinden, ek bir yazılıma gerek kalmadan yapılabilmelidir.

1.6. Sanallaştırma yazılımı merkezi yönetim, izleme, otomasyon ve birden fazla hostu tek bir noktadan kontrol edilebilmesi özelliğini desteklemelidir.

1.7. Sanallaştırma yazılımı sanal makinelere birden fazla sanal CPU atayarak yoğun iş yüklerinin yüksek performansla çalışması özelliğini desteklemelidir.

1.8. Sanallaştırma yazılımı her sanal makine için Rezervasyon, Limit ve Paylaşım seviyeleri belirleyerek kritik iş yüklerinin kaynak garantisi sağlanması özelliğini desteklemelidir.

1.9. Sanallaştırma yazılımı paylaşımlı sayfa yönetimi ve balonlama gibi teknolojilerle fiziksel RAM'in etkin kullanımının sağlanması özelliğini desteklemelidir.

1.10. Sanallaştırma yazılımı (GPU gibi) I/O yoğun uygulamalar için sanal makinelere doğrudan donanım erişimi sağlanması özelliğini desteklemelidir.

1.11. Sanallaştırma yazılımı her host üzerinde sanal makineler arasında ve fiziksel ağa bağlantı sağlayan yerel ağın sanallaştırılabilmesi özelliğini desteklemelidir.

1.12. Sanallaştırma yazılımı host'lar arasında merkezi yönetim ve gelişmiş ağ özellikleri (Trafik Şekillendirme vb.) sunan sanal ağ yapısını desteklemelidir.

1.13. Sanallaştırma yazılımı paylaşımlı depolama ortamlarında kullanılabilen, sanal makineler için optimize edilmiş kümelenmiş dosya sistemini desteklemelidir.

1.14. Sanallaştırma yazılımı depolama işlemlerini fiziksel depolama aygıtına aktararak host üzerindeki işlem yükünü azaltan VAAI teknolojisini desteklemelidir.

1.15. Sanallaştırma yazılımı çalışan bir sanal makineyi, hizmet kesintisi olmadan bir fiziksel host'tan diğerine taşınabilmesi özelliğini desteklemelidir.

1.16. Sanallaştırma yazılımı sanal makinelerin disk dosyalarını, sanal makine çalışırken kesintisiz olarak bir depolama biriminden diğerine taşınabilmesi özelliğini desteklemelidir.

1.17. Sanallaştırma yazılımı host arızası durumunda, o host üzerindeki sanal makinelerin otomatik olarak kümedeki başka bir host üzerinde yeniden başlatılabilmesi özelliğini desteklemelidir.

1.18. Sanallaştırma yazılımı kaynak yükünü sürekli izlemek suretiyle sanal makinelerin otomatik olarak taşınmasını sağlayarak küme içindeki kaynak dengelemesinin optimize edilmesi özelliğini desteklemelidir.

1.19. Sanallaştırma yazılımı kritik sanal makineler için aktif-aktif bir kopya oluşturarak sıfır kesinti ile veri kaybı ortadan kaldırması özelliğini desteklemelidir.

1.20. Sanallaştırma yazılımı sanal makineleri ve disklerini şifreleyerek hassas verilerin güvenliğinin sağlanabilmesi özelliğini desteklemelidir.

1.21. Sanallaştırma yazılımı binlerce sunucu, depolama ve ağ cihazını destekleyen kapsamlı bir Donanım Uyumluluk Listesi (HCL)'ye sahip olmalıdır.

1.22. Yüklenici Sanallaştırma yazılımının SVYMEDUP Sunucusu ile uyumlu ücretsiz versiyonunu sunucu üzerine kuracak, SVYMEDUP Verileri Depolama Ünitesi konfigürasyonu sonrasında gerekli entegrasyonu yapacak, SVYMEDUP Omurga Anahtar üzerinde idarenin belirleyeceği konfigürasyonlar yapılarak sanallaştırma yazılımı ile entegrasyonu sağlandıktan sonra idareye teslim edecektir.

2. Windows Server Veri Merkezi(Data Center) Lisansı (2 Adet)

2.1. Lisans paketi server işletim sisteminin en güncel versiyonu için teklif edilmelidir.

2.2. Lisans paketi en az 16 adet core lisansını içerecek şekilde teklif edilmelidir.

2.3. Lisans paketi, lisanslanan tek bir fiziksel sunucu (host) üzerinde sınırsız sayıda Sanal Makine (Virtual Machine - VM) çalıştırma hakkı sağlamalıdır.

2.4. Sanallaştırma katmanında Windows Hyper-V, VMware ESXi veya muadili teknolojiler kullanıldığında, lisans paketinin sunduğu sınırsız sanal kullanım hakkı geçerli olmalıdır.

2.5. Lisans Paketi sanal makinelerin güvenliği için Shielded VM ve Host Guardian Service özelliklerini desteklemelidir.

2.6. Lisans paketinde bulunan lisanslar idarenin Microsoft Toplu Lisanslama (Volume Licensing) hesabı üzerinden veya idarenin sahip olduğu ilgili Microsoft portalı hesabından dijital olarak teslim edilmelidir.

2.7. Lisans paketindeki lisanslar "Ömür Boyu" (Perpetual) kullanım hakkına sahip olmalı, kiralama modelinde olmamalıdır.

3. Windows Server Erişim(CAL) Lisansı (200 Adet)

3.1. Erişim lisansı sunucu üzerindeki servislerden (Dosya paylaşımı, Active Directory, Yazdırma hizmetleri vb.) yararlanacak kullanıcılar için Windows Server User CAL şeklinde olmalıdır.

3.2. Erişim lisansları, "Kullanıcı Bazlı" (User-Based) olmalıdır. Bu sayede bir kullanıcı; masaüstü bilgisayar, taşınabilir bilgisayar veya tablet gibi farklı cihazlardan sunucuya eriştiğinde ek bir lisans gereksinimi oluşmamalıdır.

3.3. Erişim lisansları, idare tarafından kullanılmakta olan Windows Server Datacenter sürümleriyle tam uyumlu ve en güncel sürüm olmalıdır.

3.4. Erişim lisansları, idarenin ilgili Microsoft portali üzerinden dijital olarak teslim edilmeli ve kurum adına kaydedilmelidir.

3.5. Teslim edilen tüm erişim lisansları "Ömür Boyu" (Perpetual) kullanım hakkına sahip olmalı, kiralama modelinde olmamalıdır.

4. Teknik Çizim Yazılımı (20 Adet)

4.1. Teknik çizim yazılımı idare tarafından kullanılmakta olan Autocad LT yazılımına ek lisans olarak alınacaktır.

4.2. Yazılım en az 3 yıl kullanılabilecek şekilde teklif edilmelidir.

4.3. İdarenin Autodesk hesabına eklenerek diğer lisanslar ile birlikte yönetilecek özellikte ek lisans olarak teklif edilmelidir.

4.4. Yazılımın en güncel versiyonu kullanılabilecek şekilde lisanslar teklif edilmelidir.

4.5. Lisansların ekleneceği hesap bilgileri idare tarafından verilecektir.

5. Güvenlik Duvarı Log Analiz Yazılımı (1 Adet)

5.1. İdare tarafından kullanılmakta olan Fortigate güvenlik duvarının üreteceği logların analizi ve raporlaması için kullanılacak olan analiz yazılımıdır.

5.2. Log analiz yazılımı güvenlik duvarı ile tam uyumlu çalışmalıdır.

5.3. Log analiz yazılımı idare tarafından kullanılmakta olan FortiMail ve FortiSandbox sistemlerinden gelen log ve verileri merkezi bir arayüzde birleştirebilmeli, bu donanım/yazılımlar arasında tam entegrasyon sağlayarak uçtan uca otomatik görünürlük ve veri analizi sunmalıdır.

5.4. Log analiz yazılımı vSphere sanallaştırma platformu üzerinde çalışabilmelidir.

5.5. Log analiz yazılımının log işleme kapasitesi (Log Ingestion/Day) en az 5 GB/gün olmalıdır.

5.6. Log analiz yazılımı en az 3 yıllık olacak şekilde teklif edilmelidir.

5.7. Log analiz yazılımı güvenlik duvarı üreticisinin diğer ürünleriyle tam uyumlu olarak çalışmalıdır.

5.8. Log analiz yazılımı logların değiştirilmediğini kanıtlamak için "Log Signing" (Log İmzalama) özelliğine sahip olmalıdır

5.9. Log analiz yazılımının yönetim arayüzüne erişim; HTTPS, SSH ve konsol üzerinden güvenli bir şekilde yapılabilmelidir.

5.10. Log analiz yazılımı yönetici girişleri için Çok Faktörlü Kimlik Doğrulama (MFA) veya RADIUS/LDAP entegrasyonunu desteklemelidir.

5.11. Yüklenici, yazılımın kurulumunu, mevcut güvenlik duvarı ile entegrasyonunu ve temel raporlama ayarlarını yaparak sistemi çalışır vaziyette teslim etmelidir.

5.12. Log analiz yazılımına ait, üretici tarafından yayınlanan yazılım ve imza güncellemeleri garanti süresi boyunca ücretsiz olarak indirilebilmelidir.

Derviş DEMİRAYAK
Bilgisayar Mühendisi

Ayhan ÇAKIR
Bilgi Teknolojileri Şb. Md.

KAYSERİ BÜYÜKŞEHİR BELEDİYESİ
SİBER VATAN YETKİNLİK MERKEZİ KURULMASI TEKNİK ŞARTNAMESİ

İŞİN TANIMI : Kayseri Büyükşehir Belediyesi Sosyal Gelişmeyi Destekleme Programı kapsamında Siber Vatan Yetkinlik Merkezi kuracak olup bu bağlamda Eğitim ve Sertifikasyon Hizmeti alımı yapılacaktır.

İDARE : Kayseri Büyükşehir Belediyesi
İSTEKLİ : Teklif verecek olan gerçek veya tüzel kişi
YÜKLENİCİ : İşi yüklenecek olan gerçek veya tüzel kişi

1. EĞİTİM VE SERTİFİKASYON

1.1. Yüklenici Siber Vatan Yetkinlik Merkezi'nde idarenin ve yüklenici firmanın başvuran adaylar içerinden beraber belirleyeceği en az 90 kişiye aşağıda detayları bulunan eğitim verilmelidir.

1.2. Eğitimler en fazla 23'er kişilik gruplar halinde 4 grup şeklinde verilecektir.

1.3. Eğitimler hafta sonu verilecek olup her gün 4 saatten az olmamak kaydıyla her hafta sonu için toplamda en az 8 saat eğitim verilmelidir.

1.4. Eğitimler toplamda en az 8 hafta sonunu kapsayacak şekilde ve toplamda en az 60 saat olmalıdır.

1.5. Eğitimler konusunda uzman, eğitim ve saha tecrübesi bulunan, eğitim vereceği alanda sertifikalı eğitmenler tarafından verilmeli ve eğitmenler idare tarafından onaylanmalıdır.

1.6. Hafta sonu yapılan eğitimi pekiştirmek amacıyla eğitim katılımcılarının hafta içerisinde eğitim ve uygulama platformu üzerinde eğitimin uygulamalarını yapması planlanmalıdır.

1.7. Yüklenici hafta içi uygulamaları için uygulama platformu üzerinde gerekli uygulama ortamlarını hazırlamakla yükümlüdür.

1.8. Hafta içi uygulamalarına yardımcı olmak adına idarenin belirleyeceği 4 personele eğitimler öncesinde aşağıda detayları ifade edilen eğitim, eğitmen eğitimi, CEH ve CCNA sertifikasyon sınavına hazırlık eğitimi verilmeli, eğitimler sonrasında personellerin CEH ve CCNA sertifika sınavına girmesi sağlanmalıdır.

1.9. Yüklenici tarafında verilecek olan eğitimin içeriği şu şekilde olmalıdır;

CCNA NETWORK EĞİTİMİ İÇERİĞİ

Introduction to Networks v7.0 (ITN)

1. Günümüzde Ağlar
2. Temel Anahtar ve Uç ve Cihaz Yapılandırması
3. Protokoller ve Modeller
4. Fiziksel Katman
5. Sayı Sistemleri
6. Veri Bağlantısı Katmanı
7. Ethernet Anahtarlama
8. Ağ Katmanı
9. Adres Çözünürlüğü
10. Temel Yönlendirici Yapılandırması
11. IPv4 ve IPv6 Adresleme
12. ICMP
13. Taşıma Katmanı

Switching, Routing, and Wireless Essentials v7.0 (SRWE)

1. Temel Cihaz Yapılandırması
2. Anahtarlama Kavramları
3. VLAN
4. VLANlar Arası Yönlendirme
5. STP Kavramları
6. EtherChannel
7. DHCPv4
8. SLAAC ve DHCPv6
9. FHRP Kavramları
10. Yerel Ağ Güvenliği
11. WLAN Kavramları
12. WLAN Yapılandırması
13. Yönlendirme Kavramları
14. Statik Yönlendirme
15. Statik ve Varsayılan Yönlendirmede Sorun Giderme

Enterprise Networking, Security and Automation v7.0 (ENSA)

1. Tek Alanlı OSPFv2 Kavramları
2. Tek Alanlı OSPFv2 Yapılandırması
3. Ağ Güvenliği Kavramları
4. ACL Kavramları
5. IPv4 ACL Yapılandırması
6. IPv4 NAT
7. WAN Kavramları
8. VPN ve IPSec
9. QoS
10. Ağ Yönetimi
11. Ağ Tasarımı
12. Ağ Sorunlarını Giderme
13. Ağ Sanallaştırma
14. Ağ Otomasyonu

CEHv13 Eğitim Müfredatı

1.Temel Kavramlar

- Etik hacking ve sızma testi tanımları
- Bilgi güvenliği temelleri
- Hacking ile ilgili yasal ve etik sorunlar

2.Hacker Tipleri ve Psikolojisi

- Farklı hacker türleri (beyaz şapka, siyah şapka, gri şapka, vb.)
- Hacking psikolojisi

3.Saldırı Hazırlığı ve Planlama

- Hedef belirleme
- Bilgi toplama ve pasif toplama teknikleri
- Hedef firma hakkında ayrıntılı analiz

4. Ağ Saldırıları

- Port taraması ve servis tespiti

- Protokol analizi
- VLAN hopping, ARP spoofing, DoS/DDoS saldırıları

5. Sistem Hedefleme

- Hedef sistemlerin keşfi
- İşletim sistemleri üzerinde zafiyet tespiti
- Exploit teknikleri

6.Web Uygulama Hedefleme

- Web uygulamaları için güvenlik açıkları (SQL injection, XSS, CSRF, vb.)
- Web uygulama güvenliği testleri

7.Kablosuz Ağa Saldırılar

- Kablosuz ağların zayıflıkları
- WEP/WPA/WPA2 ve bu protokollere yönelik saldırılar
- Kablosuz ağ güvenliği belirleme ve test etme

8.Mobil Cihaz Hedefleme

- Mobil platformlar üzerindeki güvenlik açıkları
- Mobil uygulama güvenliği testleri

9.Bulut Güvenliği

- Bulut bilişim mimarileri ve güvenlik
- Bulut hizmetlerine yönelik saldırılar

10.Güvenlik Araçları ve Teknolojileri

- Sıfırıncı gün açıkları
- Popüler sızma testi araçları (Nmap, Metasploit, Burp Suite, Wireshark, vb.)
- Veri analiz araçları

11.Saldırıdan Sonra Tekrar Gözden Geçirme

- İlgili önlemler ve süreç
- Güvenlik ihlali sonrası olay yönetimi

12.Hackerlardan Korunma Yöntemleri

- Proaktif güvenlik önlemleri
- Güncel tehditlere karşı koruma stratejileri

4.10. Eğitimler tamamlandıktan sonra idare ve yüklenicinin ortak olarak belirleyeceği katılımcılar arasından seçilecek kişilere seçilmiş oldukları sertifikasyon sınavları için sınava hazırlık eğitimi verilmelidir.

4.11. Sertifikasyon sınavları için sınava hazırlık eğitimi sonrasında seçilen kişilerin seçildikleri sınava, sınav merkezinde girme imkânı sunulacaktır.

4.12. Katılımcılar arasından seçilecek 12 kişiye CCNA, 5 kişiye eCPPT, 5 kişiye eMAPT, 4 kişiye eWPTX ve 4 kişiye CEHv13 olmak üzere toplamda 30 kişiye sertifikasyon sınavına hazırlık eğitimi ve sonrasında sertifikasyon sınavına sınav merkezinde girme hakkı yüklenici tarafından verilecektir.

4.13. Yüklenicinin şehir dışında yerleşik bir firma olması durumunda eğitmenlerin tüm masrafları yükleniciye aittir.

4.14. İstekli firma siber güvenlik alanında kapsamlı eğitim ve danışmanlık hizmetlerini en az 5 yıldır veriyor olmalıdır.

Naci OZANSOY
Bilgisayar Mühendisi
Bilgi Teknolojileri Şube Müdürlüğü

Ayhan ÇAKICI
Bilgi Teknolojileri Şb.Md.V.