



T.C.  
ULUBEY KAYMAKAMLIĞI  
İlçe Millî Eğitim Müdürlüğü

Sayı :78502186/602.05-E.9937640  
Konu :Kurumlar Tarafından Alınması  
Gereken Siber Güvenlik Tedbirleri

21.09.2016

.....MÜDÜRLÜĞÜNE  
ULUBEY

Uşak İl Millî Eğitim Müdürlüğünün "Kurumlar Tarafından Alınması Gereken Siber Güvenlik Tedbirleri" konulu 19/09/2016 tarih ve 9856127 sayılı yazısı ve ekleri ilişikte gönderilmiştir.

Bilgi ve geriğini rica ederim.

Mustafa TURGUT  
İlçe Millî Eğitim Müdürü

EK :  
-Yazı (9 Sayfa)

DAĞITIM :  
-Tüm Teşkilata

  
**Gökhan CİNGİL**  
GÜÇ V.H.K.İ.  
21.09.16

Aşağı M. Arıkan Bedük C. Hükümet Konağı Ulubey/UŞAK  
Elektronik Ağ: www.ulubey64.gov.tr  
e-posta: gokhancingil@hotmail.com.tr

Ayrıntılı bilgi için: Gökhan CİNGİL V.H.K.İ  
Tel: (0 276) 716 16 54  
Faks: (0 276) 716 14 46



T.C.  
UŞAK VALİLİĞİ  
İl Milli Eğitim Müdürlüğü

Sayı : 52374337-602.05-E.9856127

19.09.2016

Konu : Kurumlar Tarafından Alınması Gereken  
Siber Güvenlik Tedbirleri

DAĞITIM YERLERİNE

İlgi : 31/08/2016 tarih ve 602.05/90 sayılı yazı.

Bakalığımız Strateji Geliştirme Başkanlığının "Kurumlar Tarafından Alınması Gereken Siber Güvenlik Tedbirleri" konulu ilgi yazısı ekte gönderilmiştir.

Bilgilerinizi ve gereğini rica ederim.

Bülent ŞAHİN  
Vali a.  
Milli Eğitim Müdürü

EKLER :

EK-1 Yazı ve Ekleri (8 Sayfa)

DAĞITIM :

-5 İlçe Kaymakamlığına (MEM)

-Mrk. İ.H.L. ve İ.H.O. Okul Müd.ne

Kurtuluş Mh. Enstitü Sk. Merkez/UŞAK  
web adres : <http://usak.meb.gov.tr>  
e-posta: [dinogretimi64@meb.gov.tr](mailto:dinogretimi64@meb.gov.tr)

Bilgi için : Aleattin KAYA V.H.K.İ.  
Tel : 0276 2233990-198  
Faks : 0276 2233989



T.C.  
MILLÎ EĞİTİM BAKANLIĞI  
Strateji Geliştirme Başkanlığı

Sayı : 66968699-602.05-90  
-<...>-E.<...>

31.08.2016  
<...>

Konu: Kurumlar Tarafından Alınması Gereken  
Siber Güvenlik Tedbirleri

İlgi : Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Haberleşme Genel Müdürlüğünün  
11.08.2016 tarihli ve 65532645-265.99/57837 sayılı yazı.

Bakanlar Kurulunun 2012/3842 sayılı Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu ile "Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak" görevi Ulaştırma Denizcilik ve Haberleşme Bakanlığına verilmiş olduğu malumunuzdur.

Bilgi ve iletişim teknolojilerinin hızla gelişmesi sebebiyle riskler ve tehditlerin günden güne çeşitlenerek arttığı, artan risk ve tehditlerin Siber Güvenliğe dolayısıyla da Ülke güvenliğine ciddi tehditler oluşturduğu gözlemlendiği ilgi yazı da belirtilmektedir.

Ülkemizde yaşanan gelişmeler sonucu kurumlarda Siber Güvenlik ile ilgili tedbirlerin alınarak ivedilikle uygulanması amacıyla ve 10 Şubat 2016 tarihli Siber Güvenlik Kurulu Kararı gereğince hazırlanan, Kurumlar tarafından alınması gereken önlemleri içeren Siber Güvenlik tedbirleri paketi yazı ekinde yer almaktadır.

İlgi yazı da bahse konu tedbirlerin Bakanlığımıza bağlı kurum ve ilişkili kuruluşlarında, gerek sistem gerekse personel düzeyinde farkındalığın artırılması amacıyla uygulanması istenilmektedir.

Bilgilerinizi ve gereğini arz/rica ederim.

27437  
MILLÎ EĞT. MÜD.  
02 Eylül 2016  
VALLİ

Veysel ERDEL  
Bakan a.  
Daire Başkanı

Ek: Yazı ve ekleri Hizmete Özel (7 sayfa)

Dağıtım:  
A Planı  
B Planı

T.C. UŞAK VALİLİĞİ MILLÎ EĞİTİM MÜDÜRLÜĞÜ	
YAYI	
TARİHİ	
Tüm birimlere Anadolu internet derinleştirilmiştir.	
ÖZEL KALEM	

8904159 / 19.08.2016



HİZMETE ÖZEL

T.C.

ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

Haberleşme Genel Müdürlüğü

11 Ağustos 2016

Sayı : 65532645-265.99/57837

Konu : Kurumlar Tarafından Alınması Gereken Siber Güvenlik Tedbirleri

MİLLÎ EĞİTİM BAKANLIĞINA

Bilindiği üzere 2012/3842 sayılı Bakanlar Kurulu Kararı ve 5809 sayılı Elektronik Haberleşme Kanunu ile "Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak" görevi Bakanlığımıza verilmiş olup bu hususta çalışmalarımız devam etmektedir.

Bilgi ve iletişim teknolojilerinin hızla gelişmekte olduğu, bu gelişmeler doğrultusunda risklerin ve tehditlerin günden güne çeşitlenerek arttığı, artan risk ve tehditlerin Siber Güvenliğe, dolayısıyla da Ülke güvenliğine ciddi tehditler oluşturduğu gözlemlenmektedir.

Gelişen bahse konu teknolojiler, edinilen tecrübeler ve Ülkemizde yaşanan gelişmeler sonucu Kurumlarda Siber Güvenlik ile ilgili tedbirlerin alınarak ivedilikle uygulanması amacıyla ve 10 Şubat 2016 tarihli Siber Güvenlik Kurulu Kararı gereğince, Kurumlar tarafından alınması gereken Siber Güvenlik tedbirleri paketi hazırlanmış olup Ek'te gönderilmektedir.

Bahse konu tedbirlerin Kurumunuz ile Kurumunuzun bağlı, ilgili ve ilişkili kuruluşlarında, gerek sistem gerekse personel düzeyinde farkındalığın artırılması amacıyla uygulanması hususunda bilgilerinizi ve gereğini arz ve rica ederim.

Dr. Özkan POYRAZ

Bakan a.

Müsteşar V.

EK:

1. Dağıtım Listesi (3 sayfa)
2. Kurumlar Tarafından Alınması Gereken Tedbirler (Hizmete Özel – 3 sayfa)

Hakkı Turaylıç Caddesi No:5 06338 Emek / Çankaya / ANKARA

Telefon: (0 312) 203 1787

E-posta: [dincer.dikici@udhb.gov.tr](mailto:dincer.dikici@udhb.gov.tr)

Faks: (0 312) 203 1885

İnternet Adresi: [www.udhb.gov.tr](http://www.udhb.gov.tr)

Ayrıntılı bilgi alınacak kişi:

Dinçer DİKİCİ

Ulaştırma ve Haberleşme Uzman Yardımcısı





**KURUMLAR TARAFINDAN ALINMASI GEREKEN TEDBİRLER**

1. Bilişim sistemlerine erişimlerde; bilişim hizmeti satın alınan firma personelinin ve kurum çalışanlarının yetkilendirilmesi ve emeklilik, istifa, işten çıkarılma, açığa alınma gibi nedenler ile ücretsiz izin, askerlik, doğum izni gibi uzun süreli işe ara vermelerde gerek firma personelinin gerekse kurum çalışanlarının sisteme erişim yetkilerinin **-gecikme olmaksızın-** dondurulması veya kaldırılması süreçleri net bir şekilde belirlenip uygulamaya konularak bu doğrultuda yetkisiz erişimlerin önüne geçilmesi,
2. Bilişim sistemlerinin kurulması veya işletilmesi nedeniyle bilişim sistemlerine ve bu sistemlerde bulunan verilere ilişkin bilgilere sahip olan bilişim hizmeti alınan firmalarla gizlilik sözleşmesi imzalanması, imzalanan gizlilik sözleşmelerinin içerik olarak yeterli güvenceyi sağlayacak doğrultuda yapılması,
3. Kurumsal SOME Kurulum ve Yönetim Rehberi'nde de belirtildiği üzere, bilgi sistemlerinin kurulması ve işletilmesi amacıyla hizmet satın alınan özel ticari işletmelerde çalışan firma personeline ilişkin güvenlik araştırmaları yapılması, kurum ve firma personeli ile bilgi sistemleri ve buradaki verilere ilişkin edindikleri bilgilerin gizliliğini koruyacaklarını ve korumamaları durumundaki yükümlülüklerini belirten bir gizlilik sözleşmesinin de imzalanması,
4. Güçlü parola oluşturulması, parolaların belli periyotlarla değiştirilmesi, parolaların gizliliğine ilişkin personelin yükümlülükleri gibi hususları içeren yazılı parola politikasının kurumda oluşturulması; kurumda bahse konu yazılı politikanın uygulamaya geçirilmesi ve oluşturulan parola politikasının personele duyurulması,
5. İki haneli veya 1111, 0000, 1234 gibi kolayca tahmin edilebilir parolalar ile ilk kez verilen parolaların değiştirilmeden kullanılması, parolanın e-posta ile iletilmesi, diğer personelle sıklıkla paylaşılması gibi bilgi güvenliği açısından önemli risk oluşturabilecek uygulamaların önlenmesi,
6. Kurumlarda farklı sistem veya uygulamalar için birbirinden bağımsız yetkilendirme mekanizmaları oluşturulmasından doğacak sorunların aşılabilmesi için merkezi kimlik yönetim/yetkilendirme sistemlerinin devreye sokulması; bu amaçla alınan yazılımların alındığı tüm sistemlere entegre edilebilecek yapıda olması (lisans kısıtlaması, teknik özelliklerinin kısıtlılığı vb. engeller teşkil etmeyen nitelikte olması),



7. Bilgi sistemlerinde kullanılan yazılımlarda ortaya çıkan hata ve açıklıkların giderilmesi amacıyla düzenli olarak yayımlanan yama programları için yama yönetimi süreçlerini açık şekilde tanımlayan **yazılı yama yönetimi politikası** oluşturularak sürecin politikaya uygun şekilde işletilmesi; yama yönetim süreçlerinin tüm sistemleri kapsamayı, kişilere bağılı ve bağımlı olmaksızın yürütülmesi,
8. Kullanım dışı kalan veya mülkiyeti devredilen, üzerine kişisel veri kaydedilmiş elektronik kayıt ortamlarının güvenli imhası ile ilgili yazılı politikanın oluşturulması, personelin politika konusunda farkındalığının da oluşturularak politikanın uygulanması,
9. Ulusal Siber Olaylara Müdahale Merkezi (USOM) tarafından gönderilen, yayımlanan ve duyurulan "Siber Güvenlik bildirimlerinin" kurumsal kullanıcılara ve sistem yöneticilerine iletilmesi ve gereğinin yapılmasının sağlanması,
10. USOM tarafından güncel biçimde sunulan "Zararlı Bağlantıların" kurumsal güvenlik cihazlarına kural olarak eklenmesi,
11. Güncel gelişmelerden hareketle önemi ortaya çıktığı üzere ve iletişim eksikliğinden doğan problemlerin tekrar yaşanmaması adına, güncel değilse SOME personeli iletişim bilgilerinin güncellenerek USOM'a bildirilmesi,
12. Kurumsal SOME Kurulum ve Yönetim rehber dokümanının "Kurumsal SOME'lerin Görev ve Sorumlulukları" başlıklı 4. kısmında bulunan (siber olay öncesi, siber olay esnası, siber olay sonrası) metin ve akış diyagramlarının gözden geçirilmesi,
13. Kurum bünyesinde mevcut kullanıcıların zombi olup olmadığının tespitinin yapılması, tespit edilememesi halinde hafta sonraları ve akşamları "kurum internet" ağının "zorunlu kullanıcılar" haricinde kullanımının önüne geçilerek bu kuralın dikkatli biçimde uygulanmasının sağlanması,
14. Olası bir siber saldırı neticesinde kurum sistemlerinin hızlı biçimde ayağa kaldırılması amacıyla gerekli **acil durum planlarının** hazırlanması,
15. Kritik altyapılar başta olmak üzere kurum ve kuruluşlar bünyesindeki sistemlerin güvenlik testlerinin (sızma testi, APT analizleri vb.) düzenli olarak yaptırılması ve analizler sonucunda tespit edilen açıklıkların **-gecikme olmaksızın-** kapatılması,
16. Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri dokümanındaki "Kamu Kurumlarının Sağlaması Gereken Kriterler" başlığı altında da belirtildiği üzere manyetik kart vb. kimlik doğrulama yöntemleri ile sistem odalarının güvenliği sağlanarak yetkisiz kişilerin girişlerinin önlenmesi,



**HİZMETE ÖZEL**

**EK**

17. Kurumsal olarak kullanılan mobil cihazların (telefon, tablet vb.) uzaktan yönetimi için MDM (Mobil Device Management – Mobil Cihaz Yönetimi) uygulamalarının kullanılması, merkezi olarak profil ve güvenlik politikalarının tanımlanmasına imkan verecek sistemlerin devreye alınması,
18. Kritik görev icra eden kamu kurum ve kuruluş personelinin çalışma ortamlarında veya görevi sırasında yanında bulundurduğu akıllı cihazın görevin gizliliğini tehlikeye düşüreceği bilinciyle hareket etmesi ve kritik konuların görüşüleceği toplantılara cep telefonu vb. akıllı cihazların alınmamasına yönelik kurumsal düzenlemelerin yapılması (Kurum girişlerindeki ziyaretçi kayıt noktalarında kilitli dolaplarda muhafaza edilmesi vb),
19. Kurum mahremiyetini içeren görüşme ve yazışmaların anlık mesajlaşma uygulamaları (Whatsapp, Viber vb.) üzerinden yapılmaması,
20. Akıllı cihazlar üzerinde kurulacak uygulamalar için verilecek izinlerin incelenerek onaylanması,
21. Uygulama kurumlarının resmi uygulama sağlayıcılarından yapılması,
22. 2016 yılı Mart ayında Kurum ve Kuruluşlarla paylaşılan 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında belirlenen eylemlerle ilgili çalışmaların Kurumlarca zamanında, titizlikle ve eksiksiz olarak yerine getirilmesi.

**Not: Siber Güvenlikle ilgili Bakanlığımız tarafından yayınlanan dokümanlara**

**[www.udhb.gov.tr/h-12-siber-guvenlik.html](http://www.udhb.gov.tr/h-12-siber-guvenlik.html) web adresinden ulaşabilirsiniz.**



**DAĞITIM LİSTESİ:**

- CUMHURBAŞKANLIĞINA
- CUMHURBAŞKANLIĞINA  
(Devlet Denetleme Kurulu)
- TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA
- BAŞBAKANLIĞA
- GENELKURMAY BAŞKANLIĞINA
- ANAYASA MAHKEMESİ BAŞKANLIĞINA
- YARGITAY BAŞKANLIĞINA
- DANIŞTAY BAŞKANLIĞINA
- SAYIŞTAY BAŞKANLIĞINA
- DIŞİŞLERİ BAKANLIĞINA
- ADALET BAKANLIĞINA
- MİLLİ SAVUNMA BAKANLIĞINA
- İÇİŞLERİ BAKANLIĞINA
- MALİYE BAKANLIĞINA
- MİLLİ EĞİTİM BAKANLIĞINA
- SAĞLIK BAKANLIĞINA
- ÇALIŞMA VE SOSYAL GÜVENLİK BAKANLIĞINA
- ENERJİ VE TABİİ KAYNAKLAR BAKANLIĞINA
- KÜLTÜR VE TURİZM BAKANLIĞINA
- AİLE VE SOSYAL POLİTİKALAR BAKANLIĞINA
- AVRUPA BİRLİĞİ BAKANLIĞINA
- BİLİM SANAYİ VE TEKNOLOJİ BAKANLIĞINA
- ÇEVRE VE ŞEHİRCİLİK BAKANLIĞINA
- EKONOMİ BAKANLIĞINA
- GENÇLİK VE SPOR BAKANLIĞINA
- GIDA TARIM VE HAYVANCILIK BAKANLIĞINA
- GÜMRÜK VE TİCARET BAKANLIĞINA
- KALKINMA BAKANLIĞINA
- ORMAN VE SU İŞLERİ BAKANLIĞINA
- MİLLİ GÜVENLİK KURULU GENEL SEKRETERLİĞİNE
- MİLLİ İSTİHBARAT TEŞKİLATI MÜSTEŞARLIĞINA
- KAMU DÜZENİ VE GÜVENLİĞİ MÜSTEŞARLIĞINA
- SAVUNMA SANAYİİ MÜSTEŞARLIĞINA
- JANDARMA GENEL KOMUTANLIĞINA
- EMNİYET GENEL MÜDÜRLÜĞÜNE
- YÜKSEKÖĞRETİM KURULU BAŞKANLIĞINA
- TÜRKİYE BİLİMSEL VE TEKNOLOJİK ARAŞTIRMA KURUMU (TÜBİTAK)
- TÜRK DİL KURUMU BAŞKANLIĞINA
- TÜRK STANDARTLARI ENSTİTÜSÜ BAŞKANLIĞINA
- DEVLET PERSONEL BAŞKANLIĞINA
- KAMU İHALE KURUMU BAŞKANLIĞINA
- RADYO VE TELEVİZYON ÜST KURULU BAŞKANLIĞINA



- TRT GENEL MÜDÜRLÜĞÜNE
- SOSYAL GÜVENLİK KURUMU BAŞKANLIĞINA
- HÂKİMLER VE SAVCILAR YÜKSEK KURULU BAŞKANLIĞINA
- UYUŞMAZLIK MAHKEMESİ BAŞKANLIĞINA
- YÜKSEK SEÇİM KURULU BAŞKANLIĞINA
- SERMAYE PİYASASI KURULU BAŞKANLIĞINA
- ENERJİ PİYASASI DÜZENLEME KURUMU BAŞKANLIĞINA
- BANKACILIK DÜZENLEME VE DENETLEME KURUMU BAŞKANLIĞINA
- MALİ SUÇLARI ARAŞTIRMA KURULU BAŞKANLIĞINA
- TÜRKİYE ATOM ENERJİSİ KURUMU BAŞKANLIĞINA
- MADEN TETKİK VE ARAMA GENEL MÜDÜRLÜĞÜNE (MTA)
- ELEKTRİK ÜRETİM A.Ş. GENEL MÜDÜRLÜĞÜNE (EÜAŞ)
- TÜRKİYE ELEKTRİK İLETİM A.Ş. GENEL MÜDÜRLÜĞÜNE (TEİAŞ)
- TÜRKİYE ELEKTRİK TİCARET VE TAAHHÜT A.Ş. GENEL MÜDÜRLÜĞÜNE (TETAŞ)
- BORU HATLARI İLE PETROL TAŞIMA A.Ş. GENEL MÜDÜRLÜĞÜNE (BOTAŞ)
- TÜRKİYE PETROLLERİ ANONİM ORTAKLIĞI GENEL MÜDÜRLÜĞÜNE (TPAO)
- TÜRKİYE KÖMÜR İŞLETMELERİ KURUMU GENEL MÜDÜRLÜĞÜNE (TKİ)
- TÜRKİYE TAŞ KÖMÜRÜ KURUMU GENEL MÜDÜRLÜĞÜNE (TTK)
- ETİ MADEN İŞLETMELERİ GENEL MÜDÜRLÜĞÜNE
- ULUSAL BORU ARAŞTIRMA ENSTİTÜSÜ BAŞKANLIĞINA (BOREN)
- AFET VE ACİL DURUM YÖNETİMİ BAŞKANLIĞINA
- TÜRK AKREDİTASYON KURUMUNA
- BİLGİ İŞLEM DAİRESİ BAŞKANLIĞINA
- TELEKOMÜNİKASYON İLETİŞİM BAŞKANLIĞI / USOM
- BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU BAŞKANLIĞINA
- SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜNE
- KARAYOLLARI GENEL MÜDÜRLÜĞÜNE
- DEVLET HAVA MEYDANLARI İŞLETMESİ GENEL MÜDÜRLÜĞÜNE
- TCDD İŞLETMESİ GENEL MÜDÜRLÜĞÜNE
- POSTA VE TELGRAF TEŞKİLATI ANONİM ŞİRKETİ GENEL MÜDÜRLÜĞÜNE
- TÜRK SAT UYDU HABERLEŞME KABLO TV VE İŞLETME ANONİM ŞİRKETİ GENEL MÜDÜRLÜĞÜNE
- KIYI EMNİYETİ GENEL MÜDÜRLÜĞÜNE
- TÜDEMSAŞ TÜRKİYE DEMİRYOLU MAKİNALARI SANAYİ ANONİM ŞİRKETİ GENEL MÜDÜRLÜĞÜNE
- TÜVASAŞ TÜRKİYE VAGON SANAYİ ANONİM ŞİRKETİ GENEL MÜDÜRLÜĞÜNE
- TÜLOMSAŞ TÜRKİYE LOKOMOTİF VE MOTOR SANAYİ ANONİM ŞİRKETİ GENEL MÜDÜRLÜĞÜNE
- ".tr" ALAN ADI YÖNETİMİNE (Nic.tr)

- ASELSAN ELEKTRONİK SAN.TİC.A.Ş.NE
- HAVELSAN HAVA ELEKTRONİK SANAYİ VE TİCARET A.Ş.NE
- TÜRK TELEKOMÜNİKASYON A.Ş. GENEL MÜDÜRLÜĞÜNE
- TURKCELL İLETİŞİM HİZMETLERİ A.Ş. GENEL MÜDÜRLÜĞÜNE
- VODAFONE TELEKOMÜNİKASYON A.Ş.NE