

Afetlerde Kamu Bilgilendirme Yönetimi, Siber Saldırıları Ve Risk Yönetimi

Dr. Buket KURUÇAY

Kırşehir Devlet Hastanesi

AFET

- 1. Çeşitli doğa olaylarının sebep olduğu yıkım
- 2. Kıran.
- 3. Çok kötü
- 4. Güzelliği ile insanı şaşkına çeviren, aklını başından alan kadın
- 5. *Tıp* hastalıkların dokularda yaptığı bozukluk.

BİLGİLENDİRMEDE AMAÇLAR

AFET ÖNCESİ ÖNLEMLER



- Okullarda doğal afetlerin anlatılması
- Afetlerle tüm halkın mücadele etmesi gerektiği bilincinin verilmesi
- İlk yardım dersleri verilmesi
- Tatbikatlar
-

AFET SIRASINDA YAPILACAKLAR



- Olaydan haberdar etmek
- Sekonder olaylar için riski azaltmak
- Afetzedelere ulaşmak
- Yakınlarına haber ulaştırmak
- Kurumları organize etmek
- Tahliye yollarını belirlemek
- Saha içinde ilk yardım merkezleri oluşturmak

AFET SONRASI İÇİN YAPILACAKLAR



- Yeniden yapılanma
- Öncelikle temel ihtiyaçların giderilmesi
- Duyarlılığın artırılması



TATBİKAT GERÇEK OLDU





ADANA'DA ÖĞRENCİ YURDUNDA FACİA



Faciadan sağ kurtulan çocuk anlattı:

"Yangın merdiveni kapısının kilitli olduğunu biliyordum; 3. kattan aşağı attım"

Bursa'daki ilkokulda sabitlenmeyen dolabın altında kalan Yusuf yoğun bakımda

20 Eylül 2017 Çarşamba, 11:42:50 Güncelleme: 12:21:41 DHA

Bursa'nın Nilüfer ilçesindeki Canaydın İlkokulu 2. sınıf öğrencisi Yusuf Ertaş'ın üzerine sınıfta bulunan 1 metre 80 santim yüksekliğindeki dolap düştü. Ağır yaralanan Yusuf yoğun bakıma alındı



İlköğretim ve liselerde müfredatta ilk ve acil
yardım dersi





ACİL DURUM TELEFONLARI

112

AMBULANS

121

TELEFON ARIZA

110

İTFAİYE

185

SU ARIZA

155

POLİS

186

ELEKTRİK ARIZA

156

JANDARMA

187

GAZ ARIZA

Aydınlıkta



Karanlıkta







YANGIN SÖNDÜRÜCÜ KULLANMA TALİMATI



YANGINDA ÖNCELİKLE
ALARM VERİN.



YANGIN SÖNDÜRÜCÜYÜ
BULUNDUĞU YERDEN
ALIP MÜDAHALE EDİN



YANGIN SÖNMEDİYSE
EN YAKIN ACİL ÇIKIŞ
KAPISINDAN BİNAYI TERK EDİN



ODALARI TERK EDERKEN
KAPILARI KAPATIN



TOPLANMA ALANINA
GİDİN YETKİLİYE
RAPOR VERİN

AFET SIRASINDA HABERLEŞME

- MOBİL HABERLEŞME ŞİRKETLERİ
- TELEVİZYON KANALLARI
- İNTERNET
- BELEDİYELER
- RADYO KANALLARI
- CAMİLER
- ELEKTRİK SİSTEMLERİ
- GÜVENLİK GÜÇLERİ
- SİREN SİSTEMLERİ

MOBİL HABERLEŞME

- Yalnızca acil yardım hizmetlerine erişim imkanı ile sınırlı değil
- Aileye bilgi vermek
- Koordine olabilmek
- Sağlık durumu
- Hastanelerin yoğunluğu ile ilgili bilgilendirme
- Kan ihtiyacı



TELEVİZYON KANALLARI

Kamu spotları ile afet duyarlandırılmasının artırılması (*şehirlerin oluşum ve gelişimi soyut bir şekilde devlete yüklenmiş olsa da mühendislerimizin , mimarlarımızın ve işçilerimizin ve daha bir çok meslek grubunun yani halkın yadsınamaz gücü)* karşılaşılabileceğimiz can ve mal kaybını minimum düzeye indirecektir.

Afetle ilgili bilgilendirme ve kamu duyuruları

Halkı yönlendirme

Halkın sakinliğini ve metanetini korumaya yönelik programlar yapmak



INTERNET



BELEDİYELER

- Afet yönetiminin kalbi mevcut risklerin azaltılmasıdır. Bunun için öncelikle afetlerde halka zarar verecek olan yapısal ve yapısal olmayan riskler belirlenir. Bu iş de yasaklar ile olmaz!



- Deprem, sel ve heyelan gibi tehlikelerin insanlara zarar vermemesi için yapısal riskler belirlenip azaltılmalı



- Afetlerden sonra belediye, kaymakamlık, vb idari kamu binaları ile birlikte hastane gibi kritik tesislerdeki techizatın da alıřır durumda olması gerekir



Müdahale ve Operasyonlar Servisi => Ulaşım Hizmetleri Grubu

- Belediye Ulaşım Daire Bşk.lığı
- TCK 1. Bölge Müdürlüğü
- TCDD 1. Bölge Müdürlüğü
- TDİ Genel Müdürlüğü
- DHMİ Havalimanı
- Başmüdürlüğü
- İl Emniyet Md.lüğü Trf.Şb.Md.
- İl Jandarma Komutanlığı
- Vapur Genel Müdürlüğü
- Otobüs Genel Müdürlüğü
- Çevre ve Şehircilik İl Md.lüğü
- Türk Hava Yolları

Yollar afetlerde kapanabileceđi
düşünölerek yerel itfaiye için su deposu



BARINMA İMKANI









RADYOLAR KANALLAR

İKAZ VE ALARM İŞARETLERİNİ ÖĞRENİNİZ

İkaz Haberi	İşareti	YAPILACAK İŞLER VE HAREKETLER		
		İçeride	Açıkta	Araçta
SARI İKAZ Taarruz İhtimali	Üç Dakika Sürekli SİREN Sesi	Alarm'a yani aşağıdaki tedbir ve hareketlere hazır ol	Alarm'a yani aşağıdaki tedbir ve hareketlere hazır ol	Alarm'a hazır ol.
KIRMIZI İKAZ (ALARM) Taarruz Tehlikesi	Üç Dakika Yükselen Alçalan SİREN Sesi	Havagazı, elektrik, su ana anahtarlarını kapa, kapı, pencere ve perdeleri ört. Teçhizatını al ve sığınağa gir.	En yakın sığınağa gir. Yoksa sağlam bir duvar, bodrum gibi veya çukur bir yere sığın.	Araçtan çık, açıkta kiler gibi hareket et.
Radyoaktif Serpinti ya da Kimyasal Taarruz Tehlikesi	Üç Dakika Sürekli Kesik Kesik SİREN Sesi Veya Radyo Yayını	Yukarıdaki hareketleri yap.	En Yakın kapalı yere gir, açık yerlerini ört	Araçta kal ve açık yerlerini ört
		SERPİNTİNİN DÖKÜLECEĞİ ZAMAN BİLDİRİLMİŞ SE, ONA GÖRE HAREKET ET.		
BEYAZ İKAZ Tehlike Geçti	Radyo, Hoparlör veya Megafon Yayını	Sığınaktan çık, gerekliyse yardım ve kurtarma çalışmalarına katıl.	Sığındığın yerden çık, gerekliyse yardım ve kurtarma çalışmalarına katıl.	Saklı durumdan çık. Radyasyon veya gazla bulaşmışsan temizlen.

Profesyonel ekipler ilk anda yanımızda olamaz!

- İlk 72 Saat: "Altın Saatler"
- Herkes, her kurum, her tehlikede ne yapacağını bilmeli!..

SİBER SALDIRILAR

- **Siber" kelimesi İngilizce "Cyber" kelimesinden uyarlanıp kullanılmaya başlayan bir kelime olup "Bilgisayar ağlarına ait olan", "İnternete ait olan", "Sanal Gerçeklik" manalarına gelmektedir.**

2014 yılında bir önceki seneye göre %48 artış gösterdi ve bu olayların dünya ekonomisine yaklaşık 400 milyar dolarlık bir maliyeti olduğu tahmin ediliyor.

Bilgi güvenliği ile ilgili tehditlerin geldiği noktayı göstermesi açısından bir başka çarpıcı istatistik de günümüzde her gün 100.000'den fazla siber olayın gerçekleşmesidir. (Kaynak: The Global State of Information Security® Survey 2015)

RİSK YÖNETİMİ

- Tehlikeyi ortadan kaldırmak veya tehlikeli bir olay ile ilgili riski azaltmak maksadıyla bir veya daha fazla kontrol tedbiri geliştirilir.
- Tedbirler geliştirilirken sadece tehlikenin kendisi değil, tehlikenin sebepleri de düşünülür. Olası senaryoların tahlil edilmesi her bir hareket tarzı için risk azaltma tedbirleri geliştirmek için uygun ortam sağlar.

- **Kalan risk, tehlikenin giderilmesi için alınan tedbirlere rağmen ortamda hâlâ mevcut olan risktir. Tehlikeleri gidermek için tedbirler belirlenip seçildiğinde tehlikeler ikinci aşamadaki gibi yeniden değerlendirilir ve risk seviyesi tekrar gözden geçirilir. Bu süreç, kalan risk seviyesi kabul edilebilir hâle gelene kadar tekrar edilir.**

- Eğer risk kabul edilebiliyorsa, riskin seviyesinin bize olan olumsuz etkisi çok az demektir. Bu tür durumlarda risklerin yönetilmesine ve risk azaltma tedbirleri alınmasına gerek yoktur. Bununla birlikte ilave yük getirmiyorsa bu riskler de yönetilebilir ve risk azaltma tedbirleri uygulanabilir.
- Şartlı kabul edilebilir ise mutlaka risk azaltma tedbirleriyle riskin seviyesi azaltılmalı ve riskin seviyesi kabul edilebilir düzeye indirilmelidir. Riskin kabul edilebilir düzeyinden kasıt, kurum yöneticisinin kabul edebileceği risk seviyesidir.

- Belirlenen bütün tedbirlere rağmen risk kabul edilebilir düzeye indirilemiyorsa, risk kabul edilemez. Bazı durumlarda risk azaltma tedbirlerine rağmen risk seviyesi, kurum yöneticisinin belirlediği riski kabul etme eşiğinin üstünde kalabilir.
- Eğer yönetici, riski bu haliyle kabul edemeyecekse bu tehlikeye maruz kalınmayacak veya bu riske daha düşük seviyede maruz kalınabilecek alternatif planlamalar yapılmalıdır.

Kurumların siber güvenlikle ilgili risklerini, ya da kısaca siber risklerini nasıl yönetebilecekleri ise risk yönetiminin dört temel yöntemi ile özetlenebilir

- Riskin Azaltılması.
- Riskin Kabul Edilmesi.
- Riskten Kaçınmak.
- Riskin Transfer Edilmesi.

En sık olarak siber sigortalar...
(Riskin transfer edilmesi)

- Bakanlıktan yapılan yazılı açıklamada, 08 Ekim 2017'de bir gazetede ki “ [Siber Sefer Emri](#)” Bakanlığın 13 bin [Siber Güvenlik Uzmanı](#) istihdam ettiğ i ve siber güvenlik amacıyla siber sefer emri çıkartılacağı na ilişkin çalışma yapıldığı ifadelerinin yer aldığı belirtildi.
- Açıklamada, yaşanabilecek siber güvenlik olaylarına karşı kamu kurumlarının hangi seviyede olduğ unun belirlenmesi ve bu konuda kurumların farkındalığ ının artırılarak gereken iyileştirmeleri yapmalarının teşvik edilmesi amacıyla 29 Kasım 2017 tarihinde Ulusal Siber Güvenlik Tatbikatı düzenleneceğ i ifade edildi.
- Açıklamada ayrıca, "5809 Sayılı Elektronik Haberleşme Kanununda ve Diğer kanunlarda Değ iş iklik Yapılmasına Dair Kanun Tasarısı Taslağ ı"nın hazırlanarak Başbakanlığ a gönderildiğ i ve yasalaş masının beklendiğ i belirtildi.

- Klasik dünyadaki silah kavramından farklı olarak siber silah sadece yok etme amacı taşımamaktadır.

Yeri geldiğinde yok etme, yeri geldiğinde iz silme ve yeri geldiğinde hedef sistemlerden bilgi kaçıрма amaçlı kullanılacak yöntem ve araçlardır.

SİBER SALDIRI EN ÇOK WEB SİTELERİNDE GÖRÜLÜYOR

Yapılan araştırmalar, örnek vaka analizleriyle farklı sektörlerdeki siber saldırılar incelendiğinde, bilgi güvenliği olaylarının %35'inin web saldırıları, %22'sinin siber casusluk ve %14'ünün satış noktası ihlalleri (POS) olduğunu gösteriyor.

TÜRKİYE'DEKİ SİBER GÜVENLİK YAPILARI VE FAALİYETLERİ

- Türkiye'deki internet kullanıcılarının bilgi güvenliği/siber güvenlik farkındalığının artırılması amacıyla TÜBİTAK BİLGEM tarafından Bilgimi Koruyorum E-Öğrenme Projesi <http://www.bilgimikoruyorum.org.tr/> adlı bir site kuruldu.
- Site, kullanıcılara sadece kendilerini korumayı öğretmeyi değil, onları siber saldırılara alet olmamak konusunda bilinçlendirmeyi de amaçlıyor.
- Ayrıca Siber Güvenlik Derneği, Bilgi Güvenliği Derneği gibi sivil toplum kuruluşları düzenledikleri konferanslar, seminerler ve eğitimlerle toplumda siber güvenlik farkındalığı oluşturuyor. Son yıllarda özellikle protesto amaçlı “hacktivizm” faaliyetlerinden büyük kamu kurumları ve özel şirketler de nasibini alıyor.
- Siber suçlara karşı uluslararası düzeydeki ilk sözleşme Avrupa Konseyi tarafından hazırlanan Siber Suç Sözleşmesi'dir. Sözleşmeyi 39 Avrupa Konseyi üyesi, ABD, Kanada, Japonya ve Güney Afrika olmak üzere toplam 43 ülkenin imzaladığı biliniyor. Türkiye de 10 kasım 2010'da Dışişleri Bakanlığı düzeyinde bu belgeyi imzalamış bulunuyor.

- 2023 yılına kadar en az üç nükleer enerji santrali inşa etmek isteyen Türkiye'nin siber saldırılara hedef olmaması için gerekli siber savunma altyapısını kurması ve hazırlıklarını yapması gerekiyor.
- Bu bağlamda yasal düzenlemelerin oluşturulması, uluslararası hukuktan kaynaklanan hakların kullanılabilmesi için hazırlık yapılması, ulusal bilgisayar olaylarına müdahale organizasyonunun kurulması, ulusal siber güvenlik altyapısının güçlendirilmesi, siber güvenlik alanında insan kaynağı yetiştirilmesi, siber güvenlikte milli teknolojilerin geliştirilmesi için seferber olunması gerekiyor.

***EN ZAYIF SİSTEMİNİZ
KADAR GÜÇLÜSÜNÜZ!!!***



***Beni görmek demek mutlaka yüzümü görmek demek değildir.
Benim fikirlerimi, benim duygularımı anlıyorsanız ve hissediyorsanız bu yeterlidir.
Cumhuriyeti, ve onun gereklerini yüksek sesle anlatınız.
Bunu yüreklere yerleştirmek için elverişli olan hiçbir durumu kaçırmayınız.***