Hayatın Kaynağı Tehlikede mi? Dijitalleşen Su Altyapıları ve Güvenlik Sorunları

Tuğrulhan TERZİ - *Bilgisayar Mühendisi*

tterzi@cbernet.com

Su Altyapılarının Kritik Rolü: Neden Hayati?

Sabah uyanıp dişlerinizi fırçalarken, kahvenizi yaparken ya da duş alırken hiç düşündünüz mü? Musluğunuzdan akan su evinize nasıl bu kadar güvenle ulaşıyor? İşte tam da bu noktada, genellikle göz ardı ettiğimiz dev bir sistem devreye giriyor: **Su Altyapıları.** Ve bu sistemler, dijital dünyada giderek daha savunmasız hale geliyor.

Su altyapıları, kamu sağlığının korunması, tarım ve sanayinin sürdürülebilirliği ve genel yaşam kalitesinin sağlanması açısından temel öneme sahiptir. İçme suyu temininden atık suyun arıtılmasına kadar uzanan bu sistemler, insan yaşamının vazgeçilmez bir parçasıdır. Örneğin yalnızca ABD'de yaklaşık 170.000 kamu su sistemi ve 16.000 atık su tesisi bulunmaktadır. Avrupa'da da benzer şekilde, milyonlarca kişiye hizmet veren entegre sistemler söz konusudur. Bu sistemlerde meydana gelecek herhangi bir kesinti, halk sağlığı ve kamu güvenliği açısından ciddi sonuçlar doğurabilir.

Bu nedenle su sistemleri, enerji şebekeleri, ulaşım altyapıları ve finans sistemleri gibi ulusal güvenlik kapsamında değerlendirilen **kritik altyapılar** arasında yer alır. Kritik altyapılar, bir ülkede toplumsal düzenin ve kamu hizmetlerinin sürdürülebilirliği için vazgeçilmez olarak tanımlanır. Avrupa Birliği'nin NIS Direktifi (Network and Information Security Directive) su altyapılarını açıkça kritik hizmet sağlayıcılar olarak sınıflandırırken, ABD Ulusal Güvenlik Ajansı (NSA) da bu sistemleri öncelikli koruma kapsamına dahil etmektedir. **Türkiye'de de Ulusal Siber Güvenlik Strateji Belgesi çerçevesinde su sistemleri kritik altyapı olarak değerlendirilmektedir.**

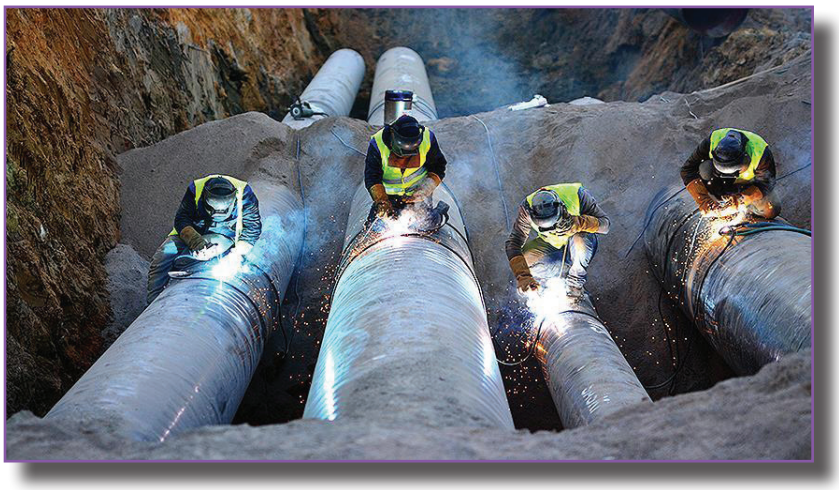
Bu önemin farkında olmak, yalnızca mühendislik veya çevre sağlığı açısından değil; aynı zamanda **siber güvenlik perspektifinden de** konuya bakmayı gerektirir. Zira fiziksel altyapıların dijitalleşmesi, siber saldırılarla kesintiye uğratılabilecek yeni zafiyetler yaratmaktadır.

Dijitalleşme: Verimlilik mi, Yeni Riskler mi?

Geçmişte arıtma tesisleri fiziksel vanalar ve manuel kontrollerle çalışırken, günümüzde bu sistemler dijital teknolojilerle yönetiliyor. **SCADA sistemleri** ile su seviyeleri uzaktan izleniyor, **IoT sensörleri** sayesinde borulardaki basınç anlık olarak takip ediliyor ve **bulut tabanlı çözümlerle** toplanan veriler analiz edilerek süreçler optimize ediliyor. Bu dönüşüm, su altyapılarında önemli bir verimlilik artışı sağlamaktadır.

Dijitalleşme sayesinde su kalitesi gerçek zamanlı izlenebiliyor, kaçaklar tespit edilebiliyor, bakım süreçleri planlanabiliyor ve operasyonel maliyetler düşürülebiliyor. Örneğin Avrupa Birliği

kaynaklı bir çalışmaya göre, dijital izleme sistemleri sayesinde su dağıtım şebekelerinde yıllık %10'a varan enerji tasarrufu sağlandığı belirtilmiştir.



Ancak bu teknolojik gelişmelerle birlikte sistemler daha karmaşık hale gelmekte ve daha geniş bir saldırı yüzeyi ortaya çıkmaktadır. Özellikle OT (Operasyonel Teknoloji) ile IT (Bilgi Teknolojisi) sistemlerinin entegrasyonu, geleneksel güvenlik önlemlerini yetersiz kılmaktadır. Endüstriyel protokoller (örneğin **Modbus, DNP3**) çoğunlukla şifreleme veya kimlik doğrulama mekanizmalarına sahip değildir. Bu durum, siber saldırganlar için ciddi bir açık oluşturmaktadır.

Ayrıca üretici firmaların sunduğu yazılım ve donanımların güncellenmemesi, zayıf parola kullanımı, internet üzerinden erişilebilen kontrol panelleri ve yetersiz erişim kontrolleri de bu altyapılarda büyük güvenlik açıklarına yol açmaktadır.

Kısacası, dijitalleşme su altyapılarını daha akıllı hale getirirken, aynı zamanda onları siber tehditlere açık bir hale getirmektedir. Bu nedenle dijital dönüşüm süreci yalnızca teknolojik gelişmelerle sınırlı kalmamalı; aynı zamanda **siber güvenlik stratejileri, risk yönetimi ve altyapı güvenliği yatırımları ile birlikte ele alınmalıdır.**

Dijitalleşmeyle Ortaya Çıkan Siber Tehditler

Dijitalleşmeyle birlikte su altyapıları, artık yalnızca doğal afetler veya fiziksel arızalarla değil; hedefli ve organize **siber saldırılarla** da karşı karşıya kalmaktadır. Bu tehditler hem teknolojik hem de insan kaynaklı olabilir. En sık karşılaşılan siber tehditler şu şekilde özetlenebilir:

1. Uzaktan Erişim İhlalleri

SCADA ve diğer kontrol sistemlerine internet üzerinden erişim sağlanması, siber saldırganlar için önemli bir fırsat yaratmaktadır. Özellikle **uzak masaüstü protokollerinin (RDP)** yanlış yapılandırılması, yetkisiz erişimlere zemin hazırlayarak doğrudan sistem müdahalelerine neden olabilir.

2. Kimlik Avı (Phishing)

Kullanılan yazılım ve donanımlardaki üretici kaynaklı açıklar, saldırganların altyapıya sızmasına olanak tanıyabilir. Özellikle yazılım güncellemelerinin yeterince denetlenmemesi ciddi riskler doğurmaktadır.

3. Fidye Yazılımları (Ransomware)

Kritik sistem dosyalarının şifrelenmesi, operasyonel faaliyetleri durma noktasına getirir. 2021 yılında ABD'de bir atık su yönetim şirketine yapılan fidye saldırısı, sistemlerin günlerce devre dışı kalmasına neden olmuştu.

4. Tedarik Zinciri Saldırıları

Kullanılan yazılım ve donanımlardaki üretici kaynaklı açıklar, saldırganların altyapıya sızmasına olanak tanıyabilir. Özellikle yazılım güncellemelerinin yeterince denetlenmemesi ciddi riskler doğurmaktadır.

5. İç Tehditler

Çalışanların kasıtlı veya ihmalkâr davranışları, dış kaynaklı tehditlerden daha büyük güvenlik açıklarına neden olabilir. Parola paylaşımı, yetkisiz veri aktarımı gibi eylemler sistem güvenliğini ciddi şekilde zayıflatmaktadır.

Bu tehditlerle etkili şekilde başa çıkabilmek için yalnızca teknik önlemler yeterli değildir. Aynı zamanda kurumsal güvenlik politikaları, personel farkındalık eğitimleri ve düzenli denetim mekanizmaları ile desteklenen bütüncül bir güvenlik yaklaşımı benimsenmelidir.

Gerçek Saldırılar: Dijital Dünyada Su Kaynaklarına Müdahale

Dijital altyapıların ne denli savunmasız olabileceğini gösteren gerçek siber vakalar, bu alandaki tehditleri daha somut ve çarpıcı hale getirmektedir:

Oldsmar, Florida (2021)

• **Olay:** Bir saldırgan, TeamViewer aracılığıyla SCADA sistemine girerek suya eklenen sodyum hidroksit dozajını **100 ppm'den 11.100 ppm'e** yükseltti

• **Süre:** İki ayrı oturumla toplamda 3–5 dakika boyunca değişiklik yapıldı.

• **Sonuç:** Operatör müdahale etti; sistem normal değere döndü. Otomatik pH alarm sistemleri henüz devreye girmeden olay durduruldu. 24–36 saat içinde tehlikeli su şebekeye ulaşabilirdi

• **Etkilenen nüfus:** Yaklaşık 15.000 kişi.

Arkansas City, Kansas (2024)

• **Olay:** Yetkisiz erişim sonrası SCADA sistemleri geçici olarak devre dışı bırakıldı.

• **Etkisi:** Su işlemleri manuel moda alındı; federal otoriteler harekete geçti.

• **Kamu sağlığı etkisi:** Hafif aksama; milyonlarca müşteriye hizmet eden sistemde sağlık riski yok.

Muleshoe, Texas (2024)

• **Olay:** "Cyber Army of Russia Reborn" adlı grubun SCADA sistemine sızarak su tankının taşmasına yol açtığı iddia edildi.

• **Nüfus:** Yaklaşık 5.000 kişilik bir kasaba.

• **Sonuç:** Tank taşması gerçekleşti; ancak erişim anında kesilerek su kesintisi yaşanmadı.

Tipton, Indiana (2023)

• **Olay:** Rusya bağlantılı bir grup atık su tesisine sızdı; bu durum çalışanların fark etmesiyle manuel moda geçiş sağlandı.

• **Popülasyon:** Yaklaşık 5.000 kişi.

• **Etkisi:** Sistem işletmeye devam etti, içme suyu etkilenmedi.

Aliquippa, Pennsylvania (2023)

• **Olay:** İran bağlantılı "CyberAv3ngers" grubu, basınç kontrol sistemlerini hedef aldı

• **Sonuç:** Pompa sistemleri durdu, kısa süreli basınç düşüşü yaşandı. Altyapı güvenlik önlemleri güçlendirildi.

Norveç (2021)

• **Olay:** Ryuk fidye yazılımı Volue'a sızdı; bu saldırıdan yaklaşık **200 su sağlayıcısı** etkilendi .

• **Etki:** Operasyonel aksama yaşandı; tedarikçi tabanlı işleri vuran bir tedarik zinciri saldırısı olarak dikkat çekti.

Bu vakaların ortak özellikleri; saldırıların çoğunun **hedefli siber kampanyalar, SCADA sistemlerine yönelik uzaktan erişim, ve fiziksel sistemlere doğrudan zarar görebilecek sonuçlara** sahip olmasıdır. Örneğin Oldsmar'da neredeyse 111 kat fazla kostik soda dozajı tehlike oluşturmuş, Muleshoe'da ise fiziki altyapıya zarar gelmiş; her iki durumda da operatörlerin hızlı müdahalesi krizi önlemiştir.

Bizim için önemli olan ders şu: Siber saldırılar sadece dijital altyapıyı değil, **insan sağlığını, çevre güvenliğini ve kamu düzenini hedef alıyor.**

Siber Güvenlik Önlemleri: Su Altyapıları Nasıl Korunmalı?

Yukarıda örnekleri verilen saldırılar, su altyapılarının siber tehditlere karşı ne denli kırılgan olduğunu açıkça göstermektedir. Bu nedenle bu sistemlerin yalnızca teknik değil; **stratejik, ekonomik ve insani boyutlarıyla** da korunması gerekmektedir. Aşağıda, dünya genelinde kabul görmüş iyi uygulamalara dayanan başlıca önlemler özetlenmiştir:

1. Varlık Envanteri ve Sınıflandırması

Tüm ağ bileşenlerinin, SCADA sistemlerinin, sensörlerin ve yazılımların kapsamlı bir envanteri çıkarılmalıdır. Bu varlıklar risk düzeyine göre kategorilere ayrılmalı ve önceliklendirilmelidir.

Not: *2023 yılında yapılan bir araştırmaya göre, altyapı kurumlarının %45'i kritik sistem varlıklarını güncel olarak belgelememektedir.*

2. Ağ Segmentasyonu ve Erişim Kontrolleri

Kurumsal ağ ile endüstriyel kontrol sistemleri arasına güvenlik duvarı konulmalı; yalnızca ihti-

yaç duyulan cihazlar arası iletişime izin verilmelidir. Dış erişim gerekiyorsa, VPN ve çok faktörlü kimlik doğrulama (MFA) gibi güvenli yöntemler uygulanmalıdır.

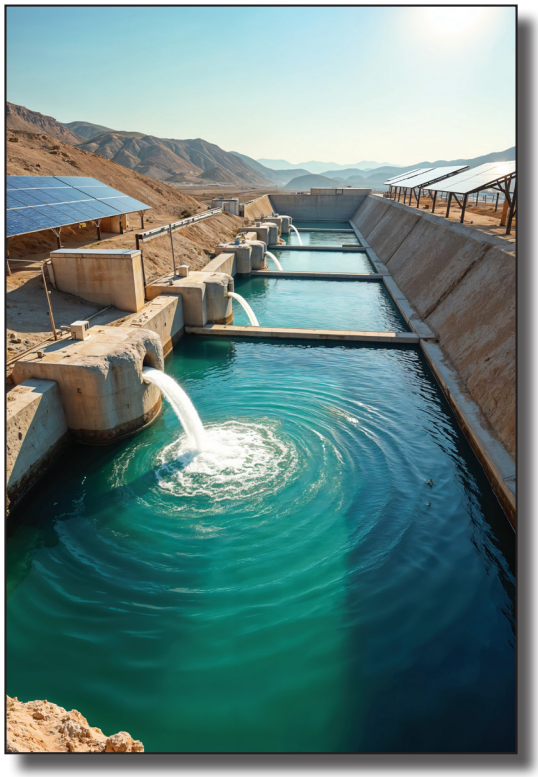
3. Güncellemeler ve Yama Yönetimi

Tüm yazılım ve firmware'ler düzenli olarak güncellenmeli, özellikle SCADA yazılımlarındaki güvenlik açıkları zamanında kapatılmalıdır.

Öneri: *Otomatik yama yerine, test edilmiş manuel yamalar tercih edilmelidir.*

4. Sıfır Güven (Zero Trust) Yaklaşımı

Kullanıcılara minimum erişim yetkisi verilmeli; tüm işlemler ve bağlantılar sürekli olarak doğrulanmalıdır. Operatör hesapları yalnızca gerektiğinde aktif hale getirilmeli ve tüm aktiviteleri denetlenmelidir.



5. İzleme, Loglama ve Anomali Tespiti

Tüm ağ trafiği ve olay günlükleri kayıt altına alınmalı; anormal davranışlar yapay zekâ destekli veya kural tabanlı sistemlerle analiz edilmelidir. OT sistemlerine özel **IDS/IPS çözümleri** (örn. Snort, Zeek, Nozomi) entegre edilmelidir

Veri: *2022'de OT sistemlerini hedef alan saldırıların %68'i daha önceden bilinmeyen davranış kalıplarıyla gerçekleşti.*

6. Personel Eğitimi ve Farkındalık Programları

Tüm teknik personel, düzenli olarak **siber hijyen, phishing farkındalığı, parola güvenliği ve sosyal mühendislik saldırıları** konusunda eğitilmelidir. Operatörlerin yalnızca teknik bilgiye değil, aynı zamanda saldırı vektörlerine karşı bilinçli bir tutuma da sahip olması gerekir.

7. İş Sürekliliği ve Olay Müdahale Planları

Her kurum, olası bir saldırı veya sistem arızası durumunda devreye alınacak bir olay müdahale planına sahip olmalı ve bu planlar düzenli olarak senaryolar üzerinden test edilmelidir.

Sonuç

Dijital dönüşüm, su altyapılarında önemli bir verimlilik artışı sağlamıştır. Ancak bu dönüşüm aynı zamanda ciddi riskleri de beraberinde getirmiştir. Florida'dan Norveç'e kadar yaşanan vakalar, küçük bir siber açığın dahi halk sağlığına ve kamu düzenine doğrudan tehdit oluşturabileceğini göstermektedir.

Günümüzde su altyapıları sadece mühendislik meselesi değil, aynı zamanda **siber güvenlik meselesidir.** Bu nedenle;

- **Tüm altyapı projeleri,** baştan itibaren sağlam bir siber güvenlik mimarisiyle birlikte planlanmalıdır.
- **İnsan faktörü** göz ardı edilmemeli; personel eğitimi ve farkındalık çalışmaları sürekli olarak güncellenmelidir.
- **Ulusal ve yerel yönetimler,** su ve enerji sistemlerini korumaya yönelik ortak politikalar ve etkili olay müdahale senaryoları geliştirmelidir.

Su, yaşamsal bir kaynaktır ve güvenliği yalnızca teknik ekiplerin değil, tüm toplumun sorumluluğundadır. Çünkü siber saldırılar artık sadece verileri değil, doğrudan yaşam kaynaklarımızı hedef alıyor.

Bu yüzden, suyun güvenliği bir dijital güvenlik meselesidir — ve bu mesele, geleceği koruma sorumluluğudur.

Kaynakça

1. Logical Systems Inc. – Cybersecurity in Industrial Control Systems.
2. Nextgov, Texas Tribune, GovTech – Water Infrastructure Cyber Incidents and Public Response.
3. StateScoop, Wired, CyberScoop – Critical Infrastructure Threat Intelligence Reports.
4. Insurance Journal – Ransomware Trends Affecting Public Utilities.
5. Dragos, Cyfirma – OT/ICS Threat Intelligence and Water Sector Vulnerability Reports.