thinktech
STM Teknolojik Düşünce Merkezi

Dijital Dayanıklılık

Teknolojinin hızla geliştiği günümüzde dijital dünya hayatımızın önemli bir parçası hâline gelirken, teknoloji ile birlikte gelişen yazılımlar da dijital dünyanın şekillenmesini sağlıyor. Ancak yapay zekâ uygulamaları, çevrimiçi hizmetler ve yaygın internet kullanımı dijital dünya için de bazı riskler barındırabiliyor. Hemen hemen herkesin bir sosyal medya hesabına, e-posta adresine ve dijital platform erişimine sahip olduğu günümüzde güvenliğin ve konforun sağlanması için **Dijital Dayanıklılık (Digital Resilience)** tanımı öne çıkan bir trend olarak görülüyor.

Özellikle dijital dönüşümün hızlandığı kuruluşlar ve bireysel kullanıcılar için dijital dayanıklılık kazanmak oldukça önemli bir gereksinim olarak ortaya çıkıyor.

Dijital Dayanıklılık Nedir?
Kurumlar ve kullanıcılar çevrimiçi deneyimler sırasında çeşitli risklerle karşılaşabiliyor. Kullanıcıları bu risklerden tamamen korumak her zaman mümkün olmuyor. Hatta bazı durumlarda gelişim için özellikle koruma sağlanması istenmiyor. Dijital risklerin nasıl tanımlanacağı ve yönetileceği, zor deneyimlerden alınacak dersler, iyileşme ve deneyimli kalabilmek bireysel gelişimin ve eylemliliğin önemli parçaları olarak göze çarpıyor.

Dijital dayanıklılık; risklerden kaçınma ve güvenlik davranışları yerine, dijital aktivasyonla yani çevrimiçi ortamda uygun fırsatlar ve zorluklarla etkileşime geçerek gelişen dinamik bir yapı olarak tanımlanabilir.

Dijital dayanıklılık öncelikle öğrenimden çok deneyime dayanıyor. Kaynaklara güvenin kazanılması, farklı çevrimiçi zorluklar üzerine fikir üretme ve ortaya çıkan risklerin fırsatlarından beslenme yoluyla oluşuyor. Kendini kontrol etme ve neyin zararlı olduğunu fark etme ile bunlara uygun şekilde tepki verme yeteneğinin geliştirilmesi dijital dayanıklılığın temel unsurlarını oluşturuyor[1].

COVID-19 salgını gibi yaşanan büyük olaylar dijital dünyada bireyler, gruplar ve kuruluşlar da dahil olmak üzere birçok farklı kurum için benzersiz ve olağanüstü zorluklar yarattı[2].

Dijital dayanıklılık, COVID-19 salgını sırasında yeni bir kavram olarak ortaya çıktı. Rusya'nın Ukrayna'yı işgal etmesi ve sonrasında Türkiye ile Suriye'de yaşanan depremlerin ardından daha da kritik hâle geldi.

1 https://www.drwg.org.uk/what-is-digital-resilience
2 https://aisel.aisnet.org/misq/vol47/iss1/14/

Dijital dayanıklılık, büyük ölçüde özel teknoloji sektörü ile kamu sektörü arasındaki yakın işbirliğine bağlı. Ortak fayda için kurumsal karar alma sürecini elinde tutan kamu ve özel sektör, günümüzün teknolojik yeniliklerinin çoğunu ve dijital altyapıların anahtarını elinde tutuyor[3].

Dijital dayanıklılık ayrıca dijital dünya kullanıcılarının;

- Dijital kimliklerini korurken çevrimiçi deneyimlerini güvenli ve sorumlu bir şekilde yönetebilmelerini,
- Çevrimiçi zararlardan korunmak için riskleri tanımlamalarını ve azaltmalarını,
- Yanlış bilgileri tespit etmek için güvenilir kaynaklar kullanmanın ve eleştirel düşünme becerilerini kullanmanın önemini anlamalarını,
- İhtiyaç duyduklarında yardım isteyebilmelerini,
- Deneyimlerinden ders almalarını ve işler ters gittiğinde toparlanmalarını sağlayabilmek için bilgi, beceri ve stratejiler geliştirme ihtiyacını özetliyor[4].

Dijital Dayanıklılık Nasıl Oluşur ve Gelişir?
Dijital dayanıklılık bireylerin çevrimiçi stresin olumsuz sonuçlarıyla başa çıkmasını ve gelişmesini sağlayacak bilgi, beceri ve güveni sağlayan güvenli ve uzmanlarca yönetilen ortamlardaki çevrimiçi etkinlikler yoluyla geliştiriliyor. Bu, bireylerin isteyebileceği veya ihtiyaç duyabileceği uygun destek ve rehberlikle birlikte sağlanabiliyor. İyileşmek ve dijital fırsatlarla yeniden etkileşime geçmek için desteğe sahip olmak da aynı derecede önemli bir konu olarak görülüyor.

Dijital dayanıklılık sabit bir durum olmadığından dinamik bir yapısı bulunuyor. İnsanlar herhangi bir zamanda çevrelerine, deneyimlerine ve koşullarına bağlı olarak daha az ya da daha çok dayanıklı olabiliyor. Ailelerin, hizmet sektöründe çalışanların, eğitimcilerin, politika yapıcıların, kamu çalışanlarının ve endüstrilerin de dijital dayanıklılığı destekleyen ve onu zayıflatmayan bir ekosisteme katkıda bulunması gerekiyor[1].

Kurumsal alanda bakıldığında ise kurumun yönetim ekibinin, dijital risk yönetimini periyodik olarak gözden geçirmesi ve mevcut dijital dayanıklılık seviyesinin daha kapsamlı risk ortamı için hâlâ uygun olup olmadığını belirlemesi gerekiyor. Kurumların dijital çağdaki tehditleri görerek, bunlarla başa çıkabileceklerinden emin olması önemli bir konu olarak görülüyor.

Aslında bu durum, kurumun dijital altyapısına göz atmak ve bunun kurumun genel dijital dayanıklılığını nasıl etkilediğini anlamak için bir fırsat yaratıyor. Bu aşama çok önemli, çünkü teknoloji güvenliği artırsa bile, artan dijital dayanıklılık her zaman gelişmeleri takip etmeyi sağlamayabiliyor. Yeni bir güvenlik girişimi, kurumun çevikliğini veya süreç bütünlüğünü tehlikeye atıyorsa potansiyel olarak genel dayanıklılığı ve rekabet gücünü de zayıflatabiliyor[5].

Dijital dayanıklılık bazı durumlarda siber güvenlikle karıştırılabiliyor. Ancak dijital dayanıklılık ve siber güvenlik birbiriyle tamamen farklı konular. Siber güvenlik, bir kurumun veya kullanıcının bilgisayar sistemlerini ve verilerini dış saldırılara karşı koruma uygulaması olarak tanımlanıyor. Kurumların veya bireylerin dijital dayanıklılığını oluşturmak ise daha sabırlı bir yaklaşım ve maksimum güvenlik taahhüdünü gerektiriyor. İleriye yönelik planlama yapmak ve potansiyel tehditlerle başa çıkmak için gerekli ekipmanı, malzemeleri ve uzmanları hazır bulundurmak, dijital dayanıklılık için risk yönetiminin esasını oluşturuyor.

3 https://www.digitaleurope.org/resources/the-digital-front-line-15-actions-to-boost-europes-digital-resilience/
4 https://hwb.gov.wales/keeping-safe-online/enhancing-digital-resilience-in-education-an-action-plan-to-protect-children-and-young-people-online/
5 https://www.bytesroute.com/glossary/digital-resilience.html

Kurumların ve bireylerin dijital dayanıklılığını artırmanın anahtarı, uzun vadeli düşünmek ve güçlü güvenlik önlemleri uygulamaktan geçiyor. Önemli olan potansiyel tehditlere karşı hazırlık yaparken proaktif olmak ve daha sonra bu hazırlıkları güçlü bir savunma oluşturmak için kullanmaktır[5].

Dijital dayanıklılığa giden yolda ilerlemek yalnızca kamu ve özel sektördeki kuruluşları potansiyel bir krize hazırlamakla kalmıyor, aynı zamanda ekonomik büyüme de yaratıyor. Ekonomiyi güçlendiren hayati yeniliklerden olan Yapay Zekâ (Artificial Intelligence -AI), Makine Öğrenmesi (Machine Learning -ML) ve Nesnelerin İnterneti (Internet of Things -IoT) dahil olmak üzere yeni gelişen teknolojilerin benimsenmesi dijital dayanıklılıkta önemli roller oynuyor. Bu gelişmiş teknoloji araçları yeni verimlilikler sağlayabiliyor, veriye dayalı kararları hızlandırabiliyor ve yeni ürün ile hizmetlerin pazara her zamankinden daha hızlı sunulmasına yardımcı olurken aynı zamanda küresel dijital ekonomiye duyulan güveni de koruyabiliyor[6].

Dijital dayanıklılığın siber güvenlik, ekonomi ve toplumsal gelişim konularında benimsenmesi bu yeni trendin güçlenmesi ve gelişmesinde büyük rol oynayabilir. Kurumsal ve bireysel bazda yapılacak ortak çalışmalar olumlu örnekler ortaya çıkarabiliyor.

Dijital Dayanıklılık Uygulama Örnekleri

Dijital dünya öncelikle ve çoğunlukla çocuklar üzerinde etkili oluyor. Yeni nesillerin elde ettiği teknolojik cihazlar ve yazılımlar beraberinde riskleri de getirdiğinden dijital dayanıklılık konusunda bu alanda da çalışmalar yapılabiliyor.

Çocukların dünyasında dijital dayanıklılığın oluşturulması için öncelikle evde ve devamında okulda maruz kaldıkları diğer ekosistemlerde yetişkin kontrollü çalışmalar yapılması gerekiyor. Bu noktada en büyük rol aileler ile öğretmenlere düşüyor. Kurumsal anlamda da oluşturulacak interaktif portallar çocukların dijital dayanıklılık konusunda geliştirilmesine fayda sağlayabiliyor[7].

Kurumsal anlamda da dijital dayanıklılığı artırmak için yedi önemli konu üzerinde duruluyor[8].

- Risk analizi oluşturmak gerekiyor. Özellikle dijital risklere karşı hazırlanacak bir risk analizi uzun vadede yol gösterici olabilir.
- Etik kuralların oluşturulması gerekiyor. Belirlenen etik kuralların bütün kullanıcılara tebliğ edilerek uyumunun da sağlanması önem arz ediyor.
- İşletme bazında proje modellerinden ürün modellerine geçilmesi öneriliyor. Dijital ürünler sürekli geliştiği için hiçbir zaman tam olarak sayılamadığından bu konuların projeden çok ürün olarak değerlendirilmesi ve sürekli olarak takibinin yapılarak yenilenmesi fayda sağlıyor.
- Bilgi bankası oluşturulması gerekiyor. Bilgi bankasına eklenen her yeni veri gelecekte daha sağlam dijital dayanıklılık modellerinin oluşturulmasına temel oluşturuyor. Oluşturulan bilgi bankasının erişilebilir, şeffaf ve hesap verilebilir olması önemli olarak görülüyor.
- Veri güvenliği ve özel verilere önem verilmesi gerekiyor. Bu noktada siber güvenlik ön plana çıkıyor.
- Dijital dayanıklılık için güçlü stratejik ortaklıklar oluşturulması gerekiyor. Dijital dayanıklılığın herkesin yararına olduğu düşünülerek oluşturulacak stratejik ortaklıklar uzun vadede gelişim avantajları sunabiliyor.
- Gelişim ve inovasyonun desteklenmesi gerekiyor. Teknoloji sürekli geliştiğinden dijital dönüşüm sürecini sürekli hâle getirip inovasyonlarla desteklediğinizde daha başarılı sonuçlar elde edilebiliyor.

6 https://www.weforum.org/agenda/2022/05/digital-resilience-building-the-economies-of-tomorrow-on-a-foundation-of-cybersecurity/
7 https://www.oecd.org/education/ceri/21st-Century-Children-Digital-Risks-and-Resilience.pdf
8 https://www.mightybytes.com/blog/digital-resilience/

Türkiye'de Dijital Dayanıklılık

Türkiye'de dijital dayanıklılık kapsamında çeşitli araştırma ve uygulamalar yapılıyor. Eskişehir İl Milli Eğitim Müdürlüğü tarafından geliştirilen Dijital Dayanıklılık Projesi bunlardan biri olarak öne çıkıyor. Dijital dayanıklılık projesi esas olarak "Dijital Çağda Çevrim İçi Dayanıklılık Geliştirme Rehberlik Programı" olarak biliniyor. Bu program Türkiye'de bu konuda geliştirilmiş ilklerden biri. Program; dijital çağda öğrenci gelişimini kolaylaştırıcı temel rehberlik hizmetleri, çeşitli dijital dünya sorunlarını ve risklerini ele almak ve yönetmek için gereken destekler, öğrencileri çevrimiçi zorluklarla iletişimsel ve sorun çözücü stratejilerle başa çıkmada ustalaşmaları için eğitmek amacıyla bireysel planlama hizmetleri ve öğrenci gelişiminde uygun destek ve kontrolü optimize etmek için sistem destek hizmetleri bileşenlerinden oluşuyor[9].

Geleceğin Dünyasında Dijital Dayanıklılığın Yeri

Benzersiz teknolojik yeniliklerin yaşandığı çağımızda, küresel olarak tüm sektörler ve ekonomilerde dijital dönüşüm hızlanarak artıyor. Dijital dayanıklılığı artırmaya kararlı olursak ve güçlü siber güvenlik önlemlerinin uygulamaya konmasını sağlarsak, önümüzdeki yıllarda iddialı bir küresel ekonomik gündemin başarısı görülebilir ve toplumlarımız Dördüncü Sanayi Devrimi'nin büyük potansiyelinin farkına daha iyi varabilir[6].

Dijital dayanıklılık genel olarak değerlendirildiğinde önce erken yaş gruplarında ve devamında kurumsal ölçekte uygulanabiliyor. Erken yaşlarda yapılan çalışmalar geleceğin dijital dünyasına daha hazır gençlerin yetişmesine fayda sağlarken, kurumların da işlerini sürdürülebilir ve güvenli hâle getirmesini sağlıyor. Bu noktada dijital dayanıklılığın bir bütün olarak uluslararası ölçekte değerlendirilmesi gerektiğinin önemi ortaya çıkıyor. Çünkü dijital dünyanın sağlıklı ve güvenli gelişimini dijital dayanıklılıkla sağlamak mümkün olabilir.

9 https://eskisehir.meb.gov.tr/www/cocuklarimizi-ve-genclerimizi-dijital-dunyanin-risklerine-karsi-direncli-olmalari-icin-dijital-dayaniklilik-projesi-gelistirildi/icerik/6494