
INTERJÚ KELETI ARTHURRAL

A FŐSZERKESZTŐ KÉRDEZ CÍMŰ ROVAT

Keleti Arthur

**Kiberbiztonsági szakértő, kibertitok
jövőkutató, író, az Informatikai
Biztonság Napja (ITBN) és az Önkéntes
Kibervédelmi Összefogás (KIBEV)
alapítója**

**ICSA: Milyen kihívásokkal szembesülnek
a kibervédelmi szakemberek a
metaverzumban?**

KA: A válaszhoz messziről indítanék, mert ennél a kérdéskörnél azt szükséges meghatározni, mi is pontosan az a metaverzum. Ez jelenleg egy definíciós probléma, mivel a technológusok hamarabb nevezik el és kezdik hypolni, mint mondjuk a tényleges meghatározások megszületnének rá. De ha úgy tekintünk a metaverzumra, mint a következő internetre, vagy a kibertérnek a következő lépcsőfokára, egy sokkal interaktívabb, emberközpontúbb, az emberrel jobban interakcióba lépő környezet kapunk. Ebbe beleérthetjük a web3-at, ami túlmutat a hagyományos weboldalakon. Mondhatni közelebb áll egy szimulációhoz, mint a két dimenziós dimenziós internet (amit leginkább nagyon olyan technológia korlátok alakítottak ki mint az- jó példa erre az email prokoll-ami, őszintén szólva, egy rémálom). Szóval először is a definíciók,

környezetek, normák meghatározása a feladat, majd azt követheti a kihívások felmérése.

ICSA: Az emberközpontúbb, közvetlenebb felület már maga lehet egy nagyobb veszélyforrás?

KA: Ezt kétféle képpen lehet nézni: a mostani webes felületek sem alkalmazkodnak teljesen az emberi normákhoz. Ezekre nincsenek kialakítva 100%-ban emberi normák. Tehát az újdonság amennyi veszélyt behoz, annyi előnye is lehet, sőt akár biztonságosabban lesz használható lesz.

ICSA: Valódi védelmi funkciókat tudnak beépíteni ezekbe a rendszerekbe?

KA: Technológiailag igen- bármibe lehet bármit. De itt is távolabbról közelítenék a válaszhoz. Mivel se normarendszer, se szabály nincs az új technológiákhoz, így azt sem tudjuk hogy ezeket ki vagy mi határozza meg vagy micsoda. Ezért biztos, hogy sokkal nagyobb veszélyek várnak ránk, mivel nem tudunk mihez és nem tudunk mivel igazodni. Sem a jog, sem a társadalomtudományok egyéb területei nem tudják ezeket a helyzeteket kezelni, nincsenek rá írott vagy íratlan szabályok és tapasztalások.

Nem raktuk ki azt a környezetet, amelyben ezeket az esetleges normákat/szabályokat a technológusoknak alkalmazni kellene. Valószínűleg majd a tech cégek ezeket saját maguknak kialakítják- mindenki a sajátját. Etikai normákat ugyan elkezdtek már kitalálni (mit illik, nem illik), de ezek nem reálisan betarthatóak és betartathatóak, és ami a legfontosabb- nem szankcionálhatóak. Már az internet normarendszerét leírni szándékozó Netikett is tulajdonképpen elbukott. A jogi terület most is nehezen és lassan dolgozik- az előzővel internetes megoldásokkal is küzd, nem hogy felzárkózzon az újhoz.

Ez a fajta világ behoz olyan új viselkedési elemeket, amikkel eddig nem találkoztunk.

Ezzel kapcsolatosan van egy friss élményem, egy VR környezetben tartott három dimenziós oktatásról. Eltekintve olyan apróságoktól, mint egy falnak masírozó alak az előadás alatt, az előadótól nem messze ült egy kutya. Senki sem tudta, hogy az mi - egy résztvevő, egy kiegészítő elem a térnek, vagy egy robot. Majd az előadás közben odaállt az előadó mellé és bámulta őt. Kínosan egy érdeklődő kérdést tett fel neki, de válasz nem érkezett, így az eredeti dilemmára - mi ez - nem érkezett válasz. Ez egy teljesen hétköznapi helyzet lesz a VR világban. Ott az a legkisebb probléma, hogy kutya-e vagy ember. A teljesen hétköznapi normarendszerek és

protokollok nem alakultak ki, így biztonsági réteg kialakítása szinte lehetetlen - azt akkor tudjuk, ha van alap normatíva -ami itt nincs.

A technológiai fejlődés lehetővé teszi, hogy valódi védelmi funkciókat építsünk be az új rendszerekbe, de ennek létrehozása garantáltan nem egyszerű folyamat. Jelenleg nincs egyértelmű normarendszer vagy szabályrendszer, amely alapján az új technológiákat értelmeznénk és kezelnénk. Ennek következtében az új technológiák veszélyeket rejtnek magukban, mivel nem tudjuk, mire kellene igazodnunk és hogyan kellene kezelni az esetleges problémákat.

A védelmi folyamatokat a tech cégek fogják kitalálni a saját felületeik védelme érdekében. Még bizonyos protokollok is kialakulnak, mint például egy avatár valakinek a sajátja-e, vagy ha ellopják és visszaélnék vele, mi a teendő. Ezekre bizonyosan lesz minden szervezetnek egy saját megoldása.

ICSA: Az AI lehet a védelem kialakításában a szakemberek segítségére?

KA: Az AI kétségtelenül segítséget nyújthat a védelem kialakításában, de azt is figyelembe kell venni, hogy az AI is csak olyan jó, mint amennyi adat áll rendelkezésére. Ha nem áll rendelkezésre elegendő adat az adott rendszerhez, akkor az AI nem fog tudni hatékony védelmi funkciókat kialakítani.

Emellett az AI rendszerek is hibázhatnak, és félreértelmezhetik a felhasználók tevékenységét, ami további biztonsági problémákat okozhat.

ICSA: Ha a tech cégek vállalják fel magukra ezeknek a védelmi rendszereknek és protokolloknak a kialakítását, akkor annak mennyi lehet a realitása, hogy ezt a felhasználók védelmében teszik és nem további adatgyűjtés céljából? Hisz most is ez az alapkoncepció.

KA: A kérdés jogos. Ezekben a kezdeményezésekben kell, hogy legyenek felhasználó védelmi törekvések, ahogyan az Apple most ezt az irányt erősíti. De tény, hogy nagy volumenben ennek a kivitelezése több hibalehetőséggel is jár. De a biztonság igenis eladási pont lett mára, és a hitelesség egyre nagyobb érték.

A Meta fizetős részénél is hamarosan látható lesz, hogy hány embernek ér többet a megbízhatóság és hitelesség, és hogy fizetnek-e érte valóban a felhasználók.

Az értéke biztos, hogy van a hitelességnek, ahogyan a biztonságnak is. A cégek figyelembe fogják venni ezt bizonyos szintig, de kétségtelen, hogy mindig az üzleti érdek fogja vezérelni őket. Éppen ezért fontos, hogy független felügyelettel és szabályozással rendelkező szervezetek figyeljék a cégek tevékenységét és biztosítsák a felhasználók védelmét.

ICSA: A fiatalok jobban ki lesznek téve a veszélyeknek?

KA: Nem gondolom. Van egy elmélet, hogy a gamerek lesznek a fő felhasználók (ebben az esetben nyilván a fiatalok jobban veszélyeztetve lesznek), de van olyan verzió is, hogy a cégek lesznek a fő fogyasztók és ők hozzák meg az igazi áttörést például a VR szemüvegek világába. Az igazi VR akkor fog megérkezni, amikor top 500 cég elkezd kiadni a VR szemüveget a dolgozóinak a meetingekre.

ICSA:A fiatalokra visszatérve. Tiltás vagy a tanítás lehet a jó eszköz felkészülni a kibertér újdonságaira?

KA:Amikor a fiatalokról beszélünk, meg kell találnunk azokat az eszközöket, amelyek segítségével felkészülhetnek a kibertér újdonságaira . Én sohasem voltam tiltás párti, a tanítás lehet a jó eszköz. Magam is 9 éves korom óta ülök gép előtt, és nagyon szeretem a technológiát. Ha ez nem lett volna, akkor én ma nem lennék sem kiberbiztonsággal sem kutatásokkal foglalkozó szakember, az biztos. Az sem lehetetlen, hogy egy másik típusú gyerekekre, majd felnőttekre lesz szükség a kibertérben, amihez meg pont ez a fajta fejlődés és tanulás kell. Nyilván értelmesen és okosan...de szerintem tanítani kell, és nekünk felnőtteknek is tanulni kell, mert gyorsabban és kreatívabban használják a fiatalok a

technológiát és ez arra kényszeríti az idősebb generációt hogy alkalmazkodjon jobban, s ne a szociális hálóba kelljen bízni, hogy ha nem tudja felvenni a versenyt. Az aktív élethez nekünk is alkalmazkodnia kell a digitális világhoz. Már az nem lesz működő képes, hogy „á én ezt már nem értem, majd foglalkozik vele a következő generáció”. Igenis a változás már itt van, és ha nem akarunk akár 40-50 évesen kiesni a körforgásból, akkor alkalmazkodnunk kell a digitális világhoz, és meg kell tanulnunk az új technológiákat

Az a helyzet, hogy most mindenkire rá van bízva hogy ki hogyan áll ehhez a fejlődéshez. Mesterséges intelligencia, robotok, meddig tart az ember. Sem egyházak, sem senki nem foglalt még állást igazán a témában, így mindenki a saját értékrendszere szerint dönti el, mit tart jónak, elfogadhatónak, alkalmazhatónak- és honnantól nem elfogadható egy gép segítsége. Mert online meeting jöhet, beültetett chip nem... bőrömnél van-e a határ, vagy kinek hol van a határ...Mert azért az agyunkban már logikailag már benne van a technológia egy ideje- csak fizikailag nem.

ICSA: Mindez morális szempontból problémás lehet. Ha ennyire ellenőrzés alá vonhatóak vagyunk - hiszen ezekhez a folyamatokhoz rengeteg adatot kell megadni -, akkor az adatvédelemmel és az egyéni szabadsággal kapcsolatos kérdések merülnek fel.

KA: Nehéz téma. Megint messziről közelítenék. Ahhoz is óriási bizalom kell, hogy neked más biológiai lények segítsenek. Támaszkodsz dolgokra, emberekre. Az definíció kérdése (ha kivesszük a bigtechet és „kémkedésüket”- mert így is bonyolult a képlet), hogy van egy technológia és az miben segít téged és valamilyen szinten beleszól az életedbe- akkor az nem is biztos hogy morális kérdés kellene hogy legyen. Azonban fontos, hogy tisztázzuk a technológia és az ember közötti viszonyt, és hogy milyen szinten engedjük meg a technológiának, hogy beleszóljon az életünkbe. A párommal való online kommunikáció és a digitális szívecskék küldése például szintén technológiai közvetítéssel történik, de a morális kérdéseket ezzel kapcsolatban általában nem vetjük fel.

Ami a tech cégek motivációját illeti, nehéz megmondani, hogy ténylegesen a felhasználók védelmében kívánják-e kialakítani ezeket a rendszereket, vagy csak az adatgyűjtés céljából teszik. Mindenesetre fontos lenne, hogy a jogszabályok és a szabályozások elegendő ellenőrzést és felügyeletet biztosítanak ahhoz, hogy az adatgyűjtés

ne sértse az egyének személyes jogait. Összességében azt lehet mondani, hogy az új technológiák fejlődése nagy kihívásokat jelent a biztonság és a védelem területén. A szabályozóknak és a tech cégeknek egyaránt nagy felelősséggel kell eljárniuk annak érdekében, hogy az új technológiák biztonságosan és hatékonyan használhatóak legyenek, és ne veszélyeztessék az egyének jogait és biztonságát.

ICSA: Nem lehet h az ember csak a kontroll hiányát félti?

KA: Biztos vagyok benne, hogy így van. Az elutasítás helyett azonban érdemes lenne közelebb kerülnünk a gépekhez és a technológiához, hogy igazán megértsük őket és ellenőrzésünk alá vonjuk őket. Úgy gondolom, hogy a technológia elutasítása azonos a fejlődésünk megállításával. Van egy mondás, miszerint tartsd az ellenségeidet közel magadhoz. Ha valamiben nem bízunk, akkor jobban meg kell ismernünk, mert lehet, hogy nem is ellenségünk. Szerintem ugyanez igaz a technológiára is.

Ha a Chat GPT rosszul válaszol valamit egy IT-snak, akkor már sejti mi romlott el benne s nem szétverni akarja, hanem máshogy megközelíteni. Szerintem ez lehet a megoldás. Teljesen mindegy amúgy, hogy hiszünk-e benne, mehetünk biológiai irányba is, amerre amúgy

eddig is mehattünk volna erre. De mi nem telepátiával kommunikálunk- mert úgy nem tudunk, hanem online beszélünk, mert erre van megoldásunk.

Szóval nem a technológiai vállalatok vették el tőlünk az embertől való kommunikációs képességet, mint például a telepátiát, mert ez a képesség sosem volt a miénk. Az online kommunikáció lehetősége azonban fejlődött és vált elérhetővé, így ezt használjuk."

ICSA: Ezek szerint fel kellene a szakembereknek is venni a kesztyűt és megoldási javaslatokat tenni, nem elutasítani és figyelni?

KA: Azt javaslom, hogy a szakemberek ne utasítsák el és ne féljenek megoldási javaslatokat tenni, hanem vegyék fel a kesztyűt és üljenek le kommunikációs szakemberekkel, jogászokkal és társadalomkutatókkal. Sajnos a mai világban a legtöbb ember nem tud kilépni a saját környezetéből, és ez a legnagyobb pofára esés az adatvédelem oldalán is. Az embereknek meg kell érteniük a felhasználói környezetet, ami jelenleg absztrakt és nehezen érthető még a szakértők számára is. A VR lehetőséget nyújthat arra, hogy a felhasználók számára érthetőbbé tegyük az adatvédelmi kérdéseket. Ha az emberek érzékelik az adatszivárgás szagát, akkor ösztönösen reagálnak és cselekednek, ezért fontos, hogy az adatvédelmi koncepciókat olyan módon tervezzük meg, hogy az emberek képesek

legyenek megérteni és reagálni rájuk. A nagy cégek profit és innováció iránti elkötelezettsége hajtja őket arra, hogy foglalkozzanak az adatvédelemmel, és az összeszedett fejlesztési folyamatok és termékek mögött nincsenek előre eltervezett összeesküvés-koncepciók. Ezért fontos, hogy mindenki tegye meg a saját kezdő lökését, és a szakemberek segítsék az embereket megérteni az adatvédelmi kérdéseket.

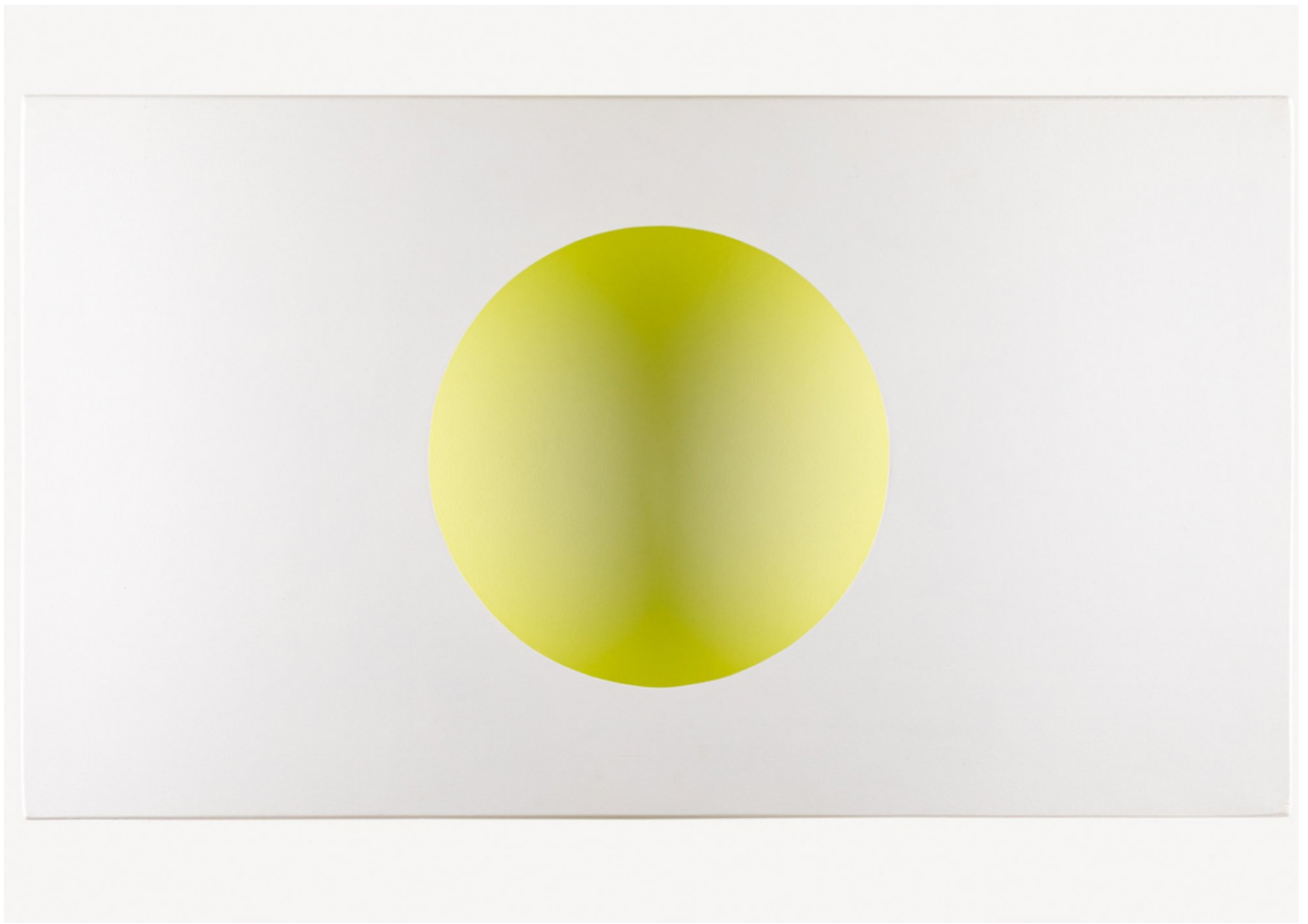
Csak a nagy cégek lépnek ez ügyben- de őket profit és innováció iránti valamiféle elköteleződés hajtja. A multicégek sem olyan összeszedetten és megkomponálva fejlesztik ki ezeket a folyamatokat és termékeket, mint mi feltételezzük- nincsenek előre eltervezett összeesküvés koncepciók. Nem megvalósítható. Egy filmkészítésnél is ahhoz, hogy jelenet úgy álljon össze, mennyi előkészület kell, és mennyi felvétel. Hogy részükről kifejezetten a szolgáltatások a biztonság és magánszféra ellen irányuljanak, az nonszensz, de nem jelenti azt hogy nem használják ki ha adódik egy lehetőség, csak az egész koncepció nem így indul sosem..

Az a kiber világ amit felépítettünk a felhasználók köré az absztrakt, az emberek nem tudják elképzelni, még néha szakértői szemmel sem. Fontos felelősség lenne számukra jobban értelmezhetővé tenni, és ez nem bizonyos biztonsági sorok kántálása.

A felhasználói környezetet tenném megérthetőbbé, s talán a VR erre egy lehetőség lesz. Például, ha adatszivárgás történik egy cégnél, akkor érezhetően bűdös lesz a levegő. Ebben az esetben reagálnak (ösztönösen), mert ha bűdös van akkor teszünk ellene. Az ember arra tud reagálni, van rá evolúciós képessége. Egy átlagfelhasználót ha szétoktatsz, hogy mit kell csinálni adatszivárgásnál, akkor sem biztos hogy csinálod, míg ha érzed a bűdöset, akkor teszel ellene valamit.

ICSA: Többször példálóztál vele, ha online beszélsz a kollégáiddal, akkor megtréfálsz őket, hogy vajon valóban veled beszélnek-e. Én honnan tudhatom, hogy ez a beszélgetés igazi volt? Veled történt?

KA: Kérdezd meg ismerőseimet, merre járhattam, és mondtam-e nekik valamit az interjúval kapcsolatban. A hitelesség és az eredet kérdése egyre fontosabbá válik. Nem azt bizonyítjuk, mi a hamisítvány, hanem mi az eredeti. Itt nyilatkoztam, és ezek az emberek tudnak róla, van bizonyítékom. Ez a jövőben egyre fontosabbá és egyre inkább hangsúlyos lesz, és erre már egyre fejlettebb technológiai eszközök állnak rendelkezésre. Ez lesz a jövő.



A kiadvány aktív támogatója a kortárs művészetnek!

No.2. magazin képeinek alkotója: Mátrai Erik

Képek forrása: <http://erikmatrai.com>

Címlap:Ablak||fa, akril||60x80x12||2015

Belső borító:Naplemente||fa, akril, polisztirol||58 x 87 cm||2014

15.o.: Glória kúp||Installáció,karton,tükrök,lámpák||40x40x40||2010

22.o.: Szpot kapu||fényinstalláció||szpot lámpák, füst||2011

40.o.: Turul||installáció||változó méret||2012

Hátsó borító: Sárga kör||fa, akril, polisztirol||50,2 x 85,7||2014

DAT'APATRON