MEĐUNARODNO POVJERENSTVO ZA TESTOVE

Smjernice o sigurnosti testova, ispita i drugih oblika procjene Međunarodnog povjerenstva za testove

6. srpnja 2014., v1.0

Završni oblik

Dokument broj: ITC-G-TS-20140706

[Hrvatski prijevod]

HRVATSKO PSIHOLOŠKO DRUŠTVO
Zagreb. 2016.

Naslov izvornika: International Test Commission, The ITC Guidelines on the Security of Tests, Examinations, and Other Assessments, 6 July, 2014, Version 1.0, Final Version, Document reference: ITC-G-TS-20140706

© 2014. International Test Commission.
All rights reserved.
Requests relating to the use, adaptation or translation of this document or any of it contents should be addressed to the Secretary-General:
Secretary@InTestC om.org
© 2016. Hrvatsko psihološko društvo, Zagreb, za djelo prevedeno na hrvatski jezik.

Smjernice o sigurnosti testova, ispita i drugih oblika procjene Međunarodnog povjerenstva za testove su prevedene uz pismeno dopuštenje prof. dr. Dragoša Iliescua, glavnog tajnika Međunarodnog povjerenstva za testove.

Sadržaj ovog dokumenta je zaštićen, a izdavačka (copyright) prava nad njime ima Međunarodno povjerenstvo za testove [*International Test Commission* (ITC)] © 2014. Sva prava pridržana. Zahtjevi vezani uz korištenje, adaptaciju ili prijevod ovog dokumenta ili bilo kojeg njegova dijela trebaju se poslati glavnom tajniku na adresu Secretary@InTestCom.org.

Formalno usvojeno

Odbor Međunarodnog povjerenstva za testove formalno je usvojio smjernice na sastanku održanom u San Sebastianu u Španjolskoj u srpnju 2014. godine.

Objavljeno na mreži

Ovaj je dokument službeno objavljen na mreži nakon Generalne sjednice Međunarodnog povjerenstva za testove održanog u San Sebastianu u Španjolskoj u srpnju 2014. godine te se otada može pronaći na mrežnoj stranici Povjerenstva: http://www.intestcom.org.

Objava u tisku

Još nije objavljena tiskana verzija ovog dokumenta.

Ovo je on-line objava.

Dokument se citira na sljedeći način:
Smjernice o sigurnosti testova, ispita i drugih oblika procjene Međunarodnog povjerenstva za testove. 6 srpnja 2014., v1.0. Završni oblik. [//Hrvatski prijevod//]. Zagreb: Hrvatsko psihološko društvo i Hrvatska psihološka komora, 2016.

Datum pristupa:
(Navesti datum pristupa)

Dostupno na:
(Odgovarajuća web adresa)

Tiskani oblik.
Smjernice će biti objavljene u tiskanom obliku u *Psihologu*, hrvatskom psihologijskom magazinu.

ZAHVALE

Ove Smjernice pripremljene su pod vodstvom dr. Davida Fostera zaposlenog u *Kryterion, Inc*. i *Caveon Test Security* (SAD), uz potporu Eugena Burkea iz *SHL*-a (VB), i Casey Marks iz *Cambridge Assessments* (SAD). Standardi su pripremljeni na temelju različitih radova i publikacija u području sigurnosti testova te bismo stoga htjeli zahvaliti nizu suradnika koji su doprinijeli ovom području, kao i onima koji su osobno sudjelovali u razvoju standarda sadržanih u ovom dokumentu. Za njihove doprinose naročito želimo zahvaliti sljedećim pojedincima:

David Bartram (Velika Britanija)

Ian Coyne (Velika Britanija)

Dragos Iliescu (Rumunjska)

Tom Oakland (Sjedinjene Američke Države)

Autor također na angažmanu i vrijednim komentarima i prijedlozima želi zahvaliti nizu članova zajednice koji su doprinijeli tijekom recenzije dokumenta: Sari Gutierrez (u ime *CEB SHL Talent Measurement*), Williamu G. Harrisu (u ime *Udruge izdavača testova*), Johnu Hattieu, Johnu Kleemanu (u ime *Questionmark*-a), Frediju Langu (u ime *Odbora za dijagnosticiranje i testove Njemačkog psihološkog društva*), Peteru Macqueenu (u ime *Skupine za testove i testiranje Australskog psihološkog društva*), Marcusu Scottu (u ime *Sigurnosti testova Caveon*), Richardu Smithu (u ime *Britanskog psihološkog društva*).

Također želimo spomenuti niz ključnih standarda i smjernica koji su nam pomogli u razvoju materijala sadržanog u ovom dokumentu. Oni uključuju:

American National Standards Institute (ANSI) (2006). *Guidance for Conformity to ANSI/ISO/IEC 17024: Requirement for Certification Program Security*.

American Educational Research Association (AERA), American Psychological Association (APA), i National Council on Measurement in Education (NCME) (1999). *Standards for Educational and Psychological Testing*.

Caveon Test Security (2009). *Test Security Standards*.

Association of Test Publishers (ATP) (2002). *Guidelines for Computer-Based Testing*.

International Test Commission (ITC) (2005). *International Guidelines on Computer-Based and Internet Delivered Testing*.

National Council on Measurement in Education (NCME) (2012). *Testing and Data Integrity in the Administration of Statewide Student Assessment Programs*.

National Organization for Competency Assurance (NOCA) (2001). *Certification Testing on the Internet*.

Želimo spomenuti i doprinos sljedećeg izvora koji je u potpunosti posvećen tematici zaštite testova i procjena:

Wollack, J. A. i Fremer, J. J. (2013). *Handbook of Test Security*. New York: Routledge.

SAŽETAK

Količina i ozbiljnost prijetnji sigurnosti značajno su se povećale tijekom posljednja dva desetljeća, čime je u pitanje dovedena i valjanost procjena koje se primjenjuju širom svijeta. Te su se prijetnje povećale zbog više razloga, koji uključuju popularno korištenje računalnih i mrežnih tehnologija za primjenu testova i korištenje gotovo neprepoznatljivih tehnologija za nelegalno preuzimanje i dijeljenje testova u različitim državama. Nijedan program procjene, bez obzira na njegovu veličinu, nije imun na ovu potencijalnu štetu.

Međunarodno povjerenstvo za testove prepoznalo je ključnu potrebu svake organizacije s razvijenim važnim programom procjene za prepoznavanjem ovakvih prijetnji i pripremu za borbu s njima. S tim su ciljem razvijene i ove Smjernice. Znanje o prijetnjama i poznavanje ovih Smjernica omogućit će razvoj učinkovitih mjera za zaštitu programa i njihovih sastavnih dijelova te održavanje vrijednosti testova i procjena u međunarodnoj zajednici.

Smjernice navedene u ovom dokumentu nude preporuke za planiranje bolje zaštite i održavanje sigurnosti tijekom razvoja i primjene testova te pripremu odgovarajućih reakcija u situacijama povrede sigurnosti. Njihovo slijeđenje može osigurati sigurnosnu granicu između onih koji namjerno varaju u procesu testiranja i vrijednih dostignuća na čiji je razvoj unutar programa utrošeno vrijeme i novac.

SADRŽAJ

ZAHVALE **3**

SAŽETAK **4**

SADRŽAJ **5**

UVOD **7**

Svrha Smjernica o sigurnosti testova i drugih oblika procjena Međunarodnog povjerenstva za testove 7

Kome su namijenjene Smjernice 7

Kako su strukturirane Smjernice o sigurnosti 8

Kako primijeniti ove Smjernice u praksi 8

SMJERNICE **9**

Djelokrug Smjernica 9

1. dio: Razvoj i implementacija sigurnosnog plana 10

2. dio: Postizanje sigurnosti procesa testiranja i procjene 15

3. dio: Odgovor na povredu sigurnosti 22

POJMOVI I DEFINICIJE **27**

LITERATURA **30**

UVOD

Svrha Smjernica o sigurnosti testova i drugih oblika procjena Međunarodnog povjerenstva za testove

Važnost potrebe za osiguravanjem testova, ispita i drugih oblika procjene povećala se paralelno s povećanjem čestine testiranja i značajnosti tehnologija u razvoju, primjeni i korigiranju/bodovanju testova, naročito putem interneta.

Svi sudionici u procesu razvoja i korištenja testova mogu se složiti s postavkom da se vrijednost rezultata testa ili drugog oblika strukturirane procjene smanjuje kada dođe do nekog oblika varanja ili krađe testa. Varanje se pritom može definirati kao bilo koji pokušaj poboljšanja rezultata na testu, ispitu ili procjeni korištenjem nepoštenih sredstava. Krađa testova se definira kao pokušaj krađe sadržaja testa prije, tijekom ili nakon njegova korištenja u predviđenu svrhu.

Temeljna svrha ovih Smjernica je prikazati ključne elemente najboljih postupaka koji omogućuju da svi sudionici koji sudjeluju u razvoju i sponzoriranju testova te ponudi usluga testiranja, kao i sami korisnici testiranja, imaju veću sigurnost prilikom primjene testova i programa procjene te obraniti vrijednost dobivenih informacija, odnosno rezultata ovih programa.

Varanje, krađa testova i drugi oblici povreda sigurnosti mogu se dogoditi čak i unutar najsavjesnijih programa. Međutim, program aktivnog upravljanja sigurnosnim rizikom osigurat će da takvih povreda bude manje te da imaju manje izražene posljedice.

Kome su namijenjene Smjernice

Mnogo je sudionika koji su uključeni u proces testiranja i procjenjivanja. Povrede sigurnosti mogu utjecati na svakog od njih te bi im poznavanje ovih Smjernica i njihova primjena mogli pomoći. Ovdje je opisano sedam skupina sudionika:

- **Pristupnici testovima.** To su pojedinci koji osobno pristupaju testovima ili drugim oblicima procjene. Te osobe mogu se registrirati, platiti i zakazati termin testiranja.
- **Osobe koje razvijaju testove.** Ovi pojedinci ili organizacije odgovorni su za konstrukciju i razvoj testova ili procjena. Oni mogu biti uključeni u širu uslugu koju nudi netko drugi.
- **Pružatelji usluga primjene testa**. Ove organizacije imaju tehnologiju i kanale distribucije (npr. centre za testiranje) koji osiguravaju da objavljeni test bude dostupan u vrijeme i na lokacijama dostupnim pristupnicima testova.
- **Pružatelji usluga zaštite testova**. Oni nude posebne sigurnosne usluge (npr. forenzičnu obradu) koje povećavaju razinu sigurnosti. Ovakve usluge mogu se nuditi u okviru većih organizacija ili neovisno o njima.

- **Pružatelji tehnoloških usluga**. Ove organizacije nude različite usluge drugim sudionicima koje uključuju, među ostalima, usluge baza podataka, banki čestica (eng. item banking), sustava komunikacije te prilagodbe i skladištenja testova.
- **Izdavači ili vlasnici testova.** Ove organizacije ili pojedinci posjeduju sadržaj testa i mogu dopustiti njegovo korištenje za specifične svrhe. U slučaju potrebe mogu se ugovorom povezati s pružateljima usluga.
- **Korisnici testova.** Korisnici testova uključuju sudionike koji koriste informacije dobivene testovima, uključujući testne rezultate, za individualno ili grupno donošenje odluka ili propisa.

Kako su strukturirane Smjernice o sigurnosti

Ove Smjernice strukturirane su prema ključnim postupcima koji su u temelju učinkovitog postizanja sigurnosti testova i procjena. Te su akcije ovako klasificirane:

- **Razvoj i implementacija sigurnosnog plana** koji opisuje potrebnu pripremu, uključujući odgovor na sigurnosne incidente te naznačava propise i procedure za aktivno upravljanje sigurnošću;
- **Postizanje sigurnosti procesa testiranja i procjene**, što uključuje i razvoj testa/procjene kao i procedure za primjenu testova i procjena; i
- **Odgovor na povredu sigurnosti** kada se otkrije varanje ili krađa testa.

Kako primijeniti ove Smjernice u praksi

Ove su Smjernice osmišljene za međunarodnu primjenu. Način njihove primjene može ovisiti o brojnim kontekstualnim uvjetima koje treba uzeti u obzir prilikom implementacije ovih Smjernice na bilo kojoj lokaciji. Ti uvjeti uključuju:

- Socijalne, političke, institucionalne, jezične i kulturalne razlike između okruženja za procjenu;
- Zakone, statute, propise, međunarodne standarde i drugu pravnu dokumentaciju koja se odnosi na problematiku testiranja:
- Zakone koji vrijede u različitim državama kroz koje podaci testiranja mogu proći, u kojima se mogu skladištiti ili koristiti; i
- Postojeće nacionalne smjernice i standarde relevantnih profesionalnih društava i udruženja.

SMJERNICE

Djelokrug Smjernica

Testne prijevare su češće u situacijama s visokim ulozima kod kojih rezultati testa, ispita ili procjene rezultiraju ishodom koji ima značajne posljedice za pristupnika testu[1] ili druge sudionike. Takve situacije uključuju obrazovne testove na temelju kojih se osigurava upis u neki odgojno-obrazovni program ili dobiva određena kvalifikacija ako se primjenjuju tijekom ili nakon takvog programa. U kliničkim okruženjima, takve situacije uključuju odlučivanje o kliničkim tretmanima ili pravnim procedurama koje ovise o dijagnozi pristupnika testu. U organizacijskom okruženju, takve situacije uključuju zapošljavanje ili napredovanje unutar organizacije. Povezane s tim su i situacije procjena vještina na temelju kojih pristupnici testovima mogu dobiti profesionalne kvalifikacije, primjerice certifikate ili dopusnice/licence. U forenzičnim okruženjima, takve situacije mogu uključivati odlučivanje o tome može li se optuženiku suditi za neki zločin ili, ako je osuđen, o visini kazne.

Dok se ove Smjernice usmjeravaju na korištenje testova, a uzimajući u obzir zrelost istraživanja i prakse vezane uz sigurnost testova, primjeri navedeni u prethodnom odjeljku pokazuju da je sigurnost problem koji se može pojaviti u bilo kojoj strukturiranoj procjeni unutar koje se vrednuje znanje, vještine, sposobnosti ili psihološke karakteristike pojedinaca. Primjerice, u organizacijskom okruženju, pristupnika se može procjenjivati putem intervjua za koji pristupnika može netko poučavati i tako ga pripremiti za pitanja koja se postavljaju na intervjuu. Promatranja ponašanja na radnom mjestu ili u učionici drugi su oblik procjene na koje mogu utjecati povrede sigurnosti, naročito ako opažač ima svoje interese vezano uz ishod promatranja. Iako se termini *test* i *ispit* češće koriste, u ovim će Smjernicama čitatelji pronaći informacije uz pomoć kojih mogu poboljšati sigurnost svih oblika procjene.

Procjene koje ne bi trebale imati visoke uloge (npr. procjena 360 stupnjeva korištena za utvrđivanje potreba za razvojem i usavršavanjem zaposlenika) mogu se pristupnicima činiti važnijima kada razumiju njihove posljedice (npr. pristupanje treningu ili programima razvoja te posljedičnu dostupnost nagrada, primjerice povećanje plaće ili napredovanje). Sudionicima će ove smjernice vjerojatno ponuditi vrijedne principe koji se mogu koristiti bez obzira na zamišljenu važnost procjene. Prepoznajući takvu općenitu vrijednost, ove smjernice ne odnose se na situacije koje ne zahtijevaju sigurnost testova, kao što su samotestiranje ili testiranje za vježbu.

1 Pristupnik i ispitanik su termini koji se često koriste kao sinonimi za opis osoba koje pristupaju testiranju, ispitu ili procjeni, bez obzira na važnost tih postupaka (tj. bez obzira na to radi li se o visokim ili niskim ulozima). U ovim Smjernicama, termin pristupnik testovima i ispitanik koriste se za opis osoba koje pristupaju bilo kojem obliku procjene, bez obzira na cilj ili važnost tih postupaka.

U ovim smjernicama često se spominje mogućnost korištenja tehnologije u prevenciji ili prepoznavanju varanja na testovima. Dok se primjena testova u velikom broju okruženja prebacila na računala i internet, sigurnost testiranja je problematika koja se odnosi na sve vrste primjene testova ili procjena. Stoga se principi opisani u ovim smjernica podjednako odnose na testove tipa papir-olovka, na modele testiranja koji se primarno oslanjaju na korištenje tehnologije, kao i na hibridne modele koji uključuju više od jednog načina testiranja. Ukratko, cilj je ovih Smjernica potaknuti postizanje sigurnosti za sve testove i procjene, bez obzira na to primjenjuju li se u situacijama s visokim ili niskim ulozima, te promovirati najbolje načine/prakse, bez obzira na to radi li se o testiranju ili procjenama tipa papir-olovka ili elektroničkim. Pritom se prepoznaje da razlike u metodama i razinama potrebne sigurnosti mogu varirati ovisno o vrsti i okruženju procjene.

Sigurnost se ne može odrediti kao pojam „sve-ili-ništa". Općenito, važno je postići ravnotežu između rizika varanja i krađa s jedne strane i, s druge strane, cijene njihova sprječavanja. Ta ravnoteža ovisi o ulozima testiranja. Ovim Smjernicama žele se opisati postupci kojima se može maksimalizirali sigurnost, pri čemu se prepoznaje kako nije nužno primijeniti sve smjernice u svim slučajevima. To upućuje na važnost provedbe analize rizika, kao i određivanje sigurnosnih mjera koje mogu smanjiti te rizike, u svakoj novoj situaciji testiranja. Također, naglašava se važnost razumijevanja sigurnosnog plana na razini cijelog procesa procjene.

Ove su Smjernice podijeljene u tri dijela: (1) Razvoj i implementacija sigurnosnog plana, (2) Postizanje sigurnosti za proces testiranja i procjene, i (3) Odgovor na povredu sigurnosti. Slijedi opis svakog od spomenutih dijelova, navedenim redoslijedom.

1. dio: Razvoj i implementacija sigurnosnog plana

Osnovna terminologija za uspješno postizanje sigurnosti uključuje pojmove prijetnji, rizika, slabosti i povreda. Priprema uspješnog programa zahtijeva znanje o postojanju specifičnih sigurnosnih prijetnji i njihovoj povezanosti s procijenjenom količinom rizika. Na primjer, ranjivost ili slabosti sustava sigurnosti, kao i neprikladno obrazovanje osoblja, povećava razinu rizika. Rizik se može izračunati neformalno, uzimajući u obzir trenutačne okolnosti koje mogu uključivati:

- vjerojatnost da će prijetnja biti uspješna,
- lakoću s kojom je moguće iskoristiti slabosti programa,
- količinu štete koju može izazvati uspješno realizirana povreda, i
- spremnost programa da prepozna/spriječi povredu i popravi štetu.

Ovi se pojmovi mogu pojasniti primjerom. Uzimajući u obzir visoke uloge državnog testiranja u SAD-u, istraživan je veliki broj sigurnosnih incidenata koji su uključivali optužbe da su neki školski administratori i nastavnici manipulirali testnim rezultatima (prijetnja) mijenjajući listove za odgovore, poučavajući učenike, nudeći učenicima pristup testovima i na druge načine (npr. dolje opisanim metodama varanja). Vjerojatnost

da će se ovo varanje zaista dogoditi i napraviti očekivanu štetu (rizik) može se unaprijed analizirati promatranjem čestine povreda u drugim državama, štete koju su te povrede izazvale i razumijevanjem činjenice da su administratori i nastavnici osobe odgovorne za primjenu testova (slabost). Povreda se događa kada se varanje dogodi i opazi.

Program koji koristi proces analize rizika i uzima u obzir ciljeve svoje organizacije, može postavljati prioritete u korištenju svojih ograničenih resursa kako bi uklonio ili smanjio prijetnje, ojačao slabosti, implementirao mehanizme detekcije koji omogućuju brzo otkrivanje pokušaja ili uspješnih povreda te se pripremio za smanjenje ili uklanjanje posljedica povreda.

Uspostava učinkovitog sigurnosnog plana zahtijeva da osoba razumije prirodu trenutačnih sigurnosnih prijetnji programa i s njima povezane rizike. Sigurnosna prijetnja je izvor potencijalnog varanja ili krađe testa. Na primjer, prijetnja varanja postoji kada se putem mobitela mogu primati tekstualne poruke tijekom testiranja. Prijetnja krađe testa postoji kada netko može pristupiti lokaciji ili uređaju za čuvanje podataka i preuzeti dio ili cijeli sadržaj testa. Potreba za uspostavljanjem i mijenjanjem učinkovitog sigurnosnog plana povećava se kako se povećava razumijevanje mogućih prijetnji i rizika vezanih uz program testiranja. Prikladno razvijen i vođen sigurnosni plan može smanjiti prijetnje i popraviti štetu uzrokovanu povredama.

Prijetnje vezane uz varanje i krađu testova prikazane su u **tablicama 1** i **2** (Foster i Miller, 2012).

Tablica 1. Kategorije prijetnji varanjem

Prijetnje varanjem	**Opis**
Korištenje predznanja o sadržaju testa	Pristupnik testu doznaje čestice u testu od pouzdanog izvora prije početka samog testiranja.
Primanje pomoći stručnjaka tijekom testiranja	Pristupnik testu prima pomoć od nastavnika ili drugog suradnika tijekom testiranja.
Korištenje nedopuštenih testnih pomagala	Pristupnik testu koristi nedopuštena pomagala tijekom testiranja, primjerice šalabahtere, mobitele, slušalice, mala računala itd.
Korištenje zamjenskog, odnosno lažnog pristupnika testu	Pristupnik testu angažira uslugu profesionalnog zamjenika ili jednostavno zamoli prijatelja ili kolegu da umjesto njega pristupi testiranju.
Manipulacija listovima za odgovore ili sačuvanim testnim rezultatima	Nakon završetka testa, osoba (npr. nastavnik) može manipulirati listovima za odgovore i ispraviti pogrešne odgovore. Također, moguće je pristupiti bazi testnih rezultata i u njoj povećati testni rezultat.
Prepisivanje odgovora od drugih pristupnika	Pristupnik testu prepisuje odgovore od drugog pristupnika tijekom testiranja.

Tablica 2. Kategorije prijetnji krađom testova.

Prijetnje krađom	**Opis**
Krađa testnih datoteka ili knjižica	Sadržaj testova je najosjetljiviji na krađu u određenim fazama distribucije testa (npr. kada se datoteke čuvaju na serveru ili testne knjižice u skladištu). Neprimjerena kontrola pristupa omogućava kradljivcima da doznaju cijeli sadržaj testa zajedno s odgovorima.
Krađa čestica u testu fotografiranjem ili kopiranjem	Testne čestice mogu se ukrasti dok se prikazuju tijekom testiranja. Kradljivac može koristiti skrivene ili neprimjetne digitalne kamere visoke rezolucije ili druge uređaje za kopiranje (npr. olovke za skeniranje).
Krađa pitanja elektroničkim snimanjem sadržaja testa	Za testove koje se primjenjuju uz pomoć modernih tehnologija, cijeli testni postupak koji uključuje sve čestice testa može se automatski sačuvati korištenjem digitalnog sustava za snimanje koji je povezan s jednim od računalnih međusklopova za izlaz podataka.
Upamćivanje sadržaja testa	Pristupnik testu može zapamtiti čestice i kasnije ih zabilježiti. Kada je dio organiziranog postupka, ovaj oblik krađe se naziva „žetva“.
Verbalno prepisivanje čestica	Usmeni ili pismeni sadržaj testa može se zabilježiti tijekom testiranja korištenjem audio ili tekstualnih uređaja za snimanje kao što su mobiteli, radioaparati (koji mogu služiti za reprodukciju i snimanje), papiri ili blokići za pisanje.
Nabava testnog materijala od osobe uključene u program	Zaposlenik ili suradnik na programu testiranja može ukrasti sadržaj testa tijekom njegova razvoja, objave ili distribucije.

Analizom rizika procjenjuje se vjerojatnost uspjeha prijetnji navedenih u tablicama 1 i 2 i šteta koja bi mogla nastati takvim povredama, što se može ilustrirati dvama primjerima.

Vjerojatno je, čak i uobičajeno, da će u svakom testnom postupku jedna osoba pokušati samostalno varati. Šteta takvog postupka je uglavnom ograničena na jednu lošu odluku zbog jednog netočnog testnog rezultata. S druge strane, ukradena testna knjižica distribuirana na internetu može neopravdano povećati tisuće ili desetke tisuća testnih rezultata. Iako su ovakvi događaji rjeđi, oni rezultiraju većom štetom. Svaka organizacija treba odrediti koliki dio svojih ograničenih resursa može izdvojiti kako bi se prepoznali, spriječili i riješili problemi pojedinačnog varanja ili odrediti procedure koje će otežati krađu i distribuciju testnih knjižica.

U tablicama 1 i 2 nabrojene su danas poznate kategorije prijetnji. Međutim, broj stvarnih *metoda* koje ljudi koriste kako bi varali ili krali unutar svake od njih broji se u stotinama. Slično kao i u bankarskoj industriji, važno je uložiti sveobuhvatne napore glede sigurnosti korištenjem višestrukih razina sigurnosnih procedura jer je dobro poznato da je kombiniranje nekoliko metoda uspješnije od jedne metode. Ove smjernice zamišljene su tako da se međusobno kombiniraju i ponude specifične upute koje će omogućiti učinkovito upravljanje sigurnosnim rizicima programa.

Specifične smjernice za razvoj i implementaciju sigurnosnog plana

Sveobuhvatni dokument koji opisuje sigurnosni plan nužan je za osiguravanje integriteta svih testova i materijala za procjenu, kao i testnih rezultata i odluka koje se na njima temelje.

1. Ovaj dokument trebao bi identificirati sigurnosne uloge i odgovornosti u svim ključnim fazama procesa, od razvoja i konstrukcije, preko implementacije do prikupljanja/čuvanja/analize rezultata te distribucije/primjene. On može pokriti neke ili sve od sljedećih uloga:
   a. Ravnatelj sigurnosti. Kada je to moguće, program bi trebao imenovati ravnatelja sigurnosti koji će biti odgovoran za sve aspekte sigurnosti programa.
   b. Odbor za sigurnost. Program bi trebao formirati odbor za sigurnost na čijem će se čelu nalaziti ravnatelj sigurnosti, a koji će uključivati pojedince odgovorne za osmišljavanje/održavanje sigurnosnog plana, procjenu ozbiljnosti i primjenu propisa vezanih uz sigurnosne incidente, nadgledanje odgovora na povrede sigurnosti i druge akcije koje će omogućiti razvoj i održavanje učinkovitog sigurnosnog plana.
   c. Rukovoditelji. Pojedinci odgovorni za razvoj i primjenu testova te prikupljanje i čuvanje rezultata testova trebali bi biti prikladno osposobljeni i pridržavati se sigurnosnih propisa i procedura definiranih u sigurnosnom planu.
   d. Prokurator, nadzornik ili osoba koja provodi testiranje. Kada predstavljaju dio sigurnosnog procesa, ovi su pojedinci odgovorni za sigurnu primjenu testa, uključujući autentifikaciju i budno motrenje pristupnika testa tijekom testiranja. Prokuratori i/ili osobe koje provode testiranje ne bi smjeli biti zaposleni kao nastavnici, stručnjaci u području testiranja, treneri ili imati druge uloge koje im omogućuju pristup sadržaju zastupljenom u testu, niti biti u drugom obliku sukoba interesa koji može utjecati na rezultate pristupnika.
   e. Pružatelji usluga sigurnosti testa. Ovi pojedinci pomažu programu u identificiranju slabosti, prevenciji sigurnosnih problema, pronalaženju povreda nakon što se dogode, određivanju nastale štete te predlaganju, a eventualno i izvedbi mogućih preporučenih akcija za njihovo uklanjanje. Ti stručnjaci za sigurnost uključuju konzultante, detektive, forenzične stručnjake, specijaliste za praćenje interneta, pravne stručnjake i druge.

2. Sigurnosni plan treba definirati prava i obveze pristupnika testiranju ili procjeni, kao i način dokumentiranja njihova prihvaćanja tih prava i obveza.
   a. Pristupnici testu imaju pravo pristupiti sigurnim procjenama s visokim ulozima u kojima nijedan drugi pristupnik testu nema nepravednu prednost zbog varanja ili drugog oblika prijevare.
   b. Pristupnici testu koji su osumnjičeni ili optuženi za prijevaru imaju pravo na obranu.
   c. Pristupnici testu ne smiju odavati sadržaj testa drugima i trebaju prijaviti takvu aktivnost ako je otkriju.
3. Svim sudionicima treba na zahtjev biti dostupan sigurnosni plan.
4. Sigurnosni plan treba uključivati akcijski plan u slučaju povrede sigurnosti koji opisuje što napraviti u takvoj situaciji. Taj bi plan trebao uključivati ciljeve, rokove, odgovorne osobe, način komunikacije, put eskalacije, pravila o dijeljenju informacija i odnosima s javnošću te specifične korektivne akcije čija ozbiljnost ovisi o osobinama incidenta ili povrede. Te akcije mogu uključivati sankcije za prijestupnike, proglašavanje rezultata nevaljanima, procedure za ponovno testiranje, izmjenu baza čestica ili testnih formi i pravne sankcije.
5. Sigurnosna pravila trebala bi biti jasno navedena u sigurnosnom planu koji bi trebao biti dostupan svim zainteresiranim sudionicima. Posljedice kršenja tih pravila trebale bi biti jasne.
6. Barem jednom godišnje prikladne skupine sudionika trebale bi odobriti i provjeriti sigurnosni plan.
7. Sigurnosnim planom trebalo bi dokumentirati sigurnosne zahtjeve za propise informacijske i komunikacijske tehnologije (IKT) te procedure za zaposlenike, suradnike i sve pružatelje usluga. Ovi zahtjevi trebali bi određivati sigurno skladištenje i pristup sadržaju testova, testnim rezultatima, drugim informacijama o testu, informacijama o pristupnicima testova te zaštitu tih informacija tijekom procesa dijeljenja i prenošenja podataka.
8. Sigurnosni plan trebao bi se referirati na zakone o zaštiti privatnosti za različite zemlje i regije u kojima se provodi testiranje. Plan bi trebao navesti načine izmjena propisa i procedura koje ovise o tim razlikama. Napori usmjereni na zaštitu pojedinaca i organizacija moraju biti usklađeni s relevantnim zakonima i propisima.
9. Treba osigurati dovoljna sredstva za implementaciju aktivnosti sigurnosne prevencije i praćenja koje su opisane u dokumentu sigurnosnog plana. Uz to, treba osigurati rezervna sredstva za reagiranje na moguće najozbiljnije povrede sigurnosti. Budžet za sigurnost trebalo bi redovito procjenjivati te po potrebi prilagoditi kako bi se uspješno moglo odgovoriti na novootkrivene prijetnje.
10. Treba napraviti materijale za sigurnosni trening posvećene ulogama i obvezama opisanima u sigurnosnom planu koji bi bili dostupni svim pojedincima uključenim u proces testiranja.

11. Treba redovito koristiti ugovor o neotkrivanju podataka i druge dokumente za sve relevantne sudionike koji uključuju pristupnike testovima, davatelje usluga i zaposlenike programa. Ovi ugovori trebaju sadržavati informacije o autorskim pravima i vlasništvu testa i sadržaja procjene, vrstama ponašanja koja se smatraju varanjem te mogućim posljedicama takvih ponašanja. Od pojedinaca treba tražiti da potpisivanjem ugovora naznače da neće odavati navedene zaštićene informacije.
12. Vlasnik testa trebao bi zaštititi autorska i izdavačka prava i pravno potvrditi svoje vlasništvo kako bi zaštitio sadržaj testa u državama u kojima će biti primjenjivan.
13. Sigurnosne procedure svih davatelja usluga treba pratiti i povremeno provjeravati kako bi se procijenila učinkovitost propisa i procedura. Tu uslugu mogu osigurati unutarnji ili vanjski sigurnosni stručnjaci.

2. dio: Postizanje sigurnosti procesa testiranja i procjene

Nakon razvoja odobrenog sigurnosnog plana, moguće je osmisliti, pripremiti, implementirati i upravljati procesom postizanja sigurnosti prije, tijekom i nakon procesa testiranja ili procjenjivanja. Važni koraci u tom procesu koji utječu na sigurnost uključuju:

- registraciju pristupnika testu
- autentifikaciju ili identifikaciju pristupnika testu
- konstrukciju testa i testnih čestica
- razvoj testa
- objavljivanje i distribuciju testa
- primjenu testa
- korigiranje/bodovanje testa
- prikupljanje i dugoročno skladištenje testnih rezultata i informacija o kandidatima,

Mnogi od ovih koraka uključuju procese koji zahtijevaju praćenje i distribuciju osjetljivih materijala među zainteresiranim sudionicima.

Specifične smjernice za postizanje sigurnosti procesa testiranja i procjene

1. Od pristupnika testovima treba zatražiti da se formalno registriraju za procjenu. Registracija i zakazivanje termina testiranja ili procjene trebala bi uključivati barem dodjelu specifičnog i jedinstvenog korisničkog imena i zaporke za svakog pristupnika.
2. U trenutku registracije ili zakazivanja termina testiranja, pristupnike treba informirati o postupku prikladne procedure autentifikacije. Pristupnici mogu biti poznati organizaciji koja organizira testiranje ili već imati isprave za tu organizaciju.

Drugi način je tražiti da pristupnici testiranju osiguraju pouzdane informacije, poput pravno valjanih osobnih dokumenata sa slikama, ili da sudjeluju u biometrijskim autentifikacijskim procedurama. U nekim procedurama testiranja, potrebno je informirati pristupnike da će u jednom trenutku nakon testiranja trebati proći proces autentifikacije (kao što je slučaj kod korištenja testova za trijažu u procesima selekcije).

3. Postupci registracije pomažu u osiguravanju da se za testiranje registriraju i termin zakažu samo kvalificirane osobe. Uvjeti za takvu kvalifikaciju mogu uključivati završenu izobrazbu, prolazak na predtestiranju ili plaćanje naknade. Ako je potrebno, moguće je uvjetovati da prije ponovnog izlaska na testiranje prođe određeno vrijeme.
   a. Ako je to dopušteno i usklađeno sa zakonima o zaštiti podataka, unutar programa moguće je pripremiti i ažurirati popis „visokorizičnih" pristupnika kojima je ograničen pristup testiranju. Taj popis treba biti dostupan i off-line i on-line sustavima za registraciju i zakazivanje termina kako bi se onemogućio ili ograničio pristup testiranju tim pojedincima, prema dogovorenim pravilima programa.
4. Treba definirati propise za ponovno testiranje kako bi se smanjila mogućnost „žetve" čestica i drugih oblika testnih prijevara. Na primjer, ne bi se smjelo dopustiti da pristupnik ponovno pristupi testu koji je „prošao" ili ponovno pristupi testu prije nego što je prošlo dovoljno vremena od prvog testiranja.
5. Registraciju pristupnika testiranju ili procjeni trebalo bi pažljivo pratiti kako bi se spriječilo pristupanje testu češće od dopuštenog, čime se smanjuju prilike za krađu čestica.
6. Treba razmotriti korištenje postupaka konstrukcije testa koji ograničavaju izloženost čestica ili mijenjaju redoslijed čestica bez promjene metrijskih karakteristika testa. Pritom treba definirati način odabira i prezentacije čestica (npr. računalno prilagodljivo testiranje, potpuno individualizirano testiranje, testovi s više razina, višestruke ekvivalentne forme), odrediti smiju li se čestice obilježiti za kasniju provjeru tijekom testa te navesti pravila za raniji prekid testiranja.
   a. Kod nekih vrsta testova moguće je prekinuti prezentaciju čestica nakon što se prikaže dovoljno pitanja na temelju kojih je moguće dobiti dovoljno pouzdan rezultat i pružiti dokaz o valjanosti (npr. količinu uključenog sadržaja) za odlučivanje, čime se sprječava nepotrebno prikazivanje dodatnih pitanja.
   b. Moguće je odrediti da prezentacija pitanja završi ili se na određeni način promijeni ako postoje indikacije da je pristupnik nemotiviran, da pokušava varati ili ukrasti pitanja, da je bolestan, umoran ili da zbog nekog drugog razloga ne može ili ne želi pružiti točnu procjenu ispitivane osobine.
7. U programima se može razmisliti o sekvencijalnom prikazivanju čestica (pitanje po pitanje) koje ne dopušta pristupnicima da prikupe i sačuvaju čestice (npr. da ih

zapamte ili digitalno sačuvaju). Neki načini konstrukcije testova i čestica su sigurniji ako ograniče ili smanje mogućnost povratka na ranije odgovorene čestice (npr. računalno prilagodljivo testiranje).

8. Izloženost sadržaju testa ili procjene treba aktivno pratiti i kontrolirati. Na primjer, moguće je pripremiti procjene u kojima odabir čestica iz banke čestica ne rezultira neplaniranom izloženošću česticama koju nije moguće pratiti.
9. Kod većih banaka čestica može biti korisno primijeniti procedure primjene testova koje povećavaju kontrolu i upravljanje korištenjem i izloženosti čestica.
10. Čestice treba osmisliti imajući u vidu potrebu za nadzorom, a možda i ograničavanjem izloženosti sadržaja. To se može napraviti na mnogo načina. Ovdje je nekoliko primjera. Važno je napomenuti da korištenje novih vrsta i alternativnih formi čestica (npr. prisilnog izbora kod samoprocjena, simulacija, multimedije, interakcija tipa *povuci-ispusti*) može zahtijevati promjene postojećih sustava za razvoj testova, oblika distribucije i sustava za skladištenje podataka.
    a. Prilikom korištenja pitanja s višestrukim odgovorima, može se razmisliti o izbjegavanju prikazivanja svih odgovora (na primjer, u jednoj verziji testa moguće je prikazati odgovore jedan po jedan dok se na pitanje odgovori točno ili netočno, dok je u drugoj verziji moguće odgovore odabirati iz veće baze odgovora, pri čemu se u oba slučaja prikazuje samo dio dostupnih višestrukih odgovora).
    b. Prilikom korištenja pitanja s višestrukim odgovora, moguće je odgovore prikazati po slučaju kako biste zbunili pristupnike koji možda imaju prethodne informacije o testu.
    c. Korištenje video- i audiosnimki, simulacija i drugih oblika medija može otežati krađu sadržaja testa i onemogućiti neke metode varanja.
11. Moguće je zahtijevati korištenje naknadne ili verifikacijske forme testa ili procjene kako bi se potvrdio rezultat prethodnog testiranja koji je primijenjen u slabije zaštićenim uvjetima. Taj proces verifikacije potrebno je provesti uz znanje i pristanak pristupnika.
12. Potrebno je odrediti stroga, statistički utemeljena vremenska ograničenja koja će omogućiti dovoljno vremena za rješavanje testa, a istovremeno smanjiti mogućnost korištenja pomagala za varanje i krađu sadržaja testa.
13. Tijekom razvoja testa važno je zaštititi sadržaj testa jer čestice i testovi često prolaze kroz veći broj faza u kojima im mogu pristupiti psihometričari, urednici, stručnjaci iz područja koje se ispituje i drugi.
    a. Čestice i testove treba zaštititi ograničavanjem pristupa samo onim pojedincima koji ih razvijaju ili kontroliraju, a i tada u ograničenom trajanju.
    b. Važno je osigurati snažne mjere pristupa (npr. korisničko ime i zaporku, ili biometrijske procedure).
    c. Treba provjeriti životopise osoba koje imaju pristup sadržaju testova i testovima, od kojih treba tražiti da potpišu stroge ugovore o neotkrivanju podataka.

d. Čestice i testove koji se zbog pregleda šalju na druge servere koje privremeno nije moguće kontrolirati treba uništiti ili ukloniti na kraju procesa provjere i prikupljanja izmjena. Takvo uklanjanje i uništavanje treba potvrditi.
e. Treba ustanoviti vlasništvo nad česticama (npr. autorska i izdavačka prava) u skladu sa specifičnim državnim zakonima i propisima.
f. Osobe uključene u proces razvoja treba osposobiti za prepoznavanje i izvještavanje o povredama sigurnosti.

14. Testove treba zaštititi tijekom razvoja, objavljivanja i distribucije.
    a. Serveri na kojima se nalazi sadržaj testova trebaju se nalaziti u profesionalnim centrima za podatke koji su certificirani u skladu s međunarodnim standardima (npr. ISO 27001 ili SSAE 16) i koji koriste IKT sigurnosne mjere (npr. vatrozid i detekcija napada).
    b. Osobe koje pripremaju testove trebaju biti pouzdane i trebaju potpisati ugovor o neotkrivanju podataka.
    c. Prilikom distribucije sadržaja testa u knjižicama ili digitalnom obliku, potrebno je zaštititi svaki korak procesa distribucije i osigurati zaštićeno skladištenje na lokacijama testiranja. Davatelji usluga tehnološki potpomognute primjene testova trebaju pratiti objavljivanje i pravovremeno ažurirati sigurnosne dodatke ovlaštenim operativnim sustavima i računalnim programima za primjenu testova.
    d. Digitalni sadržaj treba zaštititi snažnim enkripcijskim shemama, bez obzira na to treba li s udaljenog servera preuzeti cjeloviti test ili u stvarnom vremenu slati pitanje po pitanje tijekom testiranja putem interneta.
    e. Sadržaj testa koji duže vremena ostaje na serveru u centru za testiranje treba biti cijelo vrijeme zaštićen snažnom kontrolom pristupa korisnika (npr. korisničkim imenima i zaporkama) i snažnim enkripcijskim shemama.
    f. Testove bi na lokacijama testiranja trebalo zadržati što je kraće moguće, u skladu s propisima programa i primjene testova.
    g. Sadržaj testa treba ukloniti ili uništiti nakon što prestane biti potreban na mjestu testiranja. Važno je provjeriti njegovo uklanjanje ili uništenje i osigurati da se sadržaj ne može povratiti.
    h. Osobe koje rade na razvoju testa trebaju osigurati da je distribucija svih osjetljivih materijala jasno dokumentirana i da se može pratiti, što treba uključivati i povrat i/ili uništenje materijala nakon korištenja, ako je to prikladno. Takav povratak ili uništavanje treba potvrditi.
15. Metode praćenja (npr. listove za praćenje u papir-olovka ili digitalnom obliku) treba koristiti kako bi se zabilježila razdoblja kontrole, pristupa i promjena datoteka.
16. Pristupnici testovima trebaju razumjeti sigurnosna pravila i posljedice njihova kršenja prije registracije i zakazivanja termina testiranja.

a. Znatno prije samog testiranja potrebno je objasniti pristupnicima (npr. možda u formularu kojim se traži pristanak i opisuju etički aspekti testiranja) da će se prije početka testa od njih zahtijevati da pročitaju i potvrde da razumiju sigurnosna pravila te daju suglasnost da će se ponašati u skladu s tim pravilima.
b. Treba jasno definirati posljedice kršenja sigurnosnih pravila.
c. Pristupnici trebaju imati priliku pristati ili odbiti pristati na poštovanje pravila prije početka testiranja. Osobe koje ne pristanu na pravila, ne bi smjele pristupiti testu.
d. Treba pripremiti i objasniti dokumentaciju koja opisuje prava pristupnika testu.

17. Ako to dopuštaju važeći zakoni, važno je autentificirati[2] pristupnike testovima. To se može provesti prije, tijekom ili nakon testiranja. Primjerene metode autentifikacije uključuju pokazivanje službene isprave sa slikom, korištenje biometrijskih uređaja poput uređaja za uzimanje otiska prstiju, dlana ili skeniranje zjenice, praćenje dinamike korištenja tastature ili korištenje metoda prepoznavanja lica.
18. Tijekom primjene i nakon autentifikacije, testovi se nalaze pod povećanim rizikom. Na primjer, u tom je razdoblju moguće ukrasti prikazane čestice ili varati na drugi način. Uz ranije dogovorene napore tijekom faza planiranja i razvoja, potrebno je uložiti dodatni trud kako bi se osiguralo, koliko je to moguće, da sadržaj testa ne bude ukraden i da se minimalizira vjerojatnost varanja[3].
    a. U sklopu sustava primjene testa treba koristiti programe za zaključavanje ili sigurne preglednike koji osiguravaju operacijski sustav i stanicu za testiranje te ograničavaju pristup vanjskim izvorima samo na materijale potrebne za dovršavanje testa.
    b. Prokuratori mogu imati mogućnost pokretanja testa korištenjem posebnih tipki koje osigura program za primjenu testa. Slične tipke mogu biti dostupne i pristupniku testa, tako da se test može pokrenuti samo aktiviranjem obiju tipki.
    c. Prokuratori trebaju pažljivo pratiti pristupnike a da ih ne ometaju. Ako to dopuštaju važeći zakoni, praćenje je moguće organizirati izdaleka, odnosno putem mreže (preko računalnih kamera), ili lokalno (na mjestu testiranja i/ili putem kamere).
    d. Prokuratori trebaju imati minimalan ili nikakav pristup monitoru pristupnika ili stranicama knjižice testa tijekom testiranja.
    e. Prokuratori bi trebali poznavati očekivane metode varanja i krađe testa te biti osposobljeni za situacije povrede sigurnosti, što uključuje pripremu izvještaja o neregularnostima tijekom testiranja.

2 Autentifikacija nije isto što i identifikacija. Kod procjena s visokim ulozima nije nužno identificirati osobu. Samo je važno osigurati da testu pristupi ista osoba koja se registrirala i pristupila programu.

3 Varanje se neizbježno može i hoće dogoditi, čak i kada postoje najučinkovitije sigurnosne mjere. Cilj je sigurnosnog programa smanjiti posljedice krađe testova i čestinu varanja dovesti na prihvatljivu razinu.

f. Prokuratori trebaju biti dovoljno motivirani da pokušaju uočiti probleme sigurnosti i da se suoče s pristupnicima testa u slučaju povrede.
g. Prokuratori ne bi smjeli biti u sukobu interesa ili osobno zainteresirani za ishod testiranja. Oni ne bi smjeli biti nastavnici pristupnika niti bi smjeli biti upoznati sa sadržajem testiranja.
h. Ako to dopuštaju važeći zakoni, trebalo bi postaviti kamere koje će pomoći u praćenju, snimanju i čuvanju snimke testiranja i bilo kakvih sigurnosnih incidenata.
i. Ako je to moguće i dopušteno važećim zakonima, prije početka testiranja trebalo bi oduzeti uređaje koji mogu omogućiti varanje ili krađu testa (npr. mobitele, tablete, kamere, papire) te ih vratiti nakon testiranja.
j. Važno je pažljivo organizirati pauze tijekom testiranja. Nakon pauze, pristupnici ne bi smjeli imati pristup pitanjima na koja su odgovarali prije pauze.
k. Nakon testiranja trebalo bi prikupiti podijeljene korištene papire s kojima se treba postupati u skladu s važećim propisima programa.
l. Ako se tijekom testiranja primijeti varanje ili krađa sadržaja testa, važno je reagirati brzo i učinkovito, u skladu sa specifičnim uputama programa za testiranje. To može uključivati privremeni prekid ili trajno otkazivanje testiranja, zapljenu korištene opreme ili materijala te pripremu službenog izvještaja o sigurnosnim neregularnostima.

19. Kada se digitalni testni rezultati prikupljaju s udaljenih servera, prebacivanje podataka treba uslijediti što prije nakon testiranja ili nakon popunjavanja svake čestice kod testova koji se primjenjuju na internetu. Podatke koji se nalaze na udaljenim serverima treba zaštititi definiranjem jasnih procedura pristupa te osigurati snažnu enkripciju tijekom prijenosa.
20. Testove i čestice treba redovito analizirati kako bi se utvrdili pokušaji varanja ili kompromitiranja testova. Osobine testa mijenjaju se nakon krađe, dijeljenja čestica ili varanja. Ovo su neki primjeri:
    a. Neuobičajeni obrazac odgovaranja (npr. netočni odgovori na lagana i točni odgovori na teška pitanja) može upućivati na varanje ili krađu.
    b. Neuobičajeno vrijeme odgovaranja za cijeli test ili čestice (npr. neuobičajeno kratko ili dugo vrijeme) može upućivati na povredu sigurnosti ili neki drugi problem.
    c. Previše tragova brisanja na testovima papir-olovka, naročito ako se radi o promjeni netočnih u točne odgovore, može upućivati na poučavanje ili manipulaciju.
    d. Neuobičajena sličnost odgovora među parovima ili skupinama pristupnika može upućivati na poučavanje, organizirano varanje ili pristup testiranju od strane neovlaštene osobe koja zamjenjuje pristupnika.

e. Neuobičajena sličnost obrazaca odgovora ili latencije odgovora među parovima ili skupinama pristupnika može upućivati na poučavanje, organizirano varanje, pristup testiranju od strane neovlaštene osobe koja zamjenjuje pristupnika ili poučavanje.

f. Neuobičajeno poboljšanje rezultata pojedinca ili skupine pristupnika od jednog do drugog dijela testiranja može upućivati na varanje.

g. Neuobičajene promjene karakteristika čestica (npr. statističkih parametara čestica) mogu upućivati na to da je čestica kompromitirana. Takve čestice treba odmah zamijeniti.

h. Različite mjerne karakteristike jedne skupine čestica na testu u usporedbi s drugima mogu upućivati da su pristupnici bili unaprijed upoznati s testom. Na primjer, usporedba rezultata na česticama koje se nazivaju „trojanski konji" (čestice koje namjerno imaju drugačije odgovore) ili ubačenim česticama (koje su po definiciji manje izložene) s izvedbom na česticama koje se regularno boduju može upućivati da su pristupnici bili unaprijed upoznati s testom.

i. Ako to dopuštaju važeći zakoni, mogu se analizirati demografski podaci pristupnika testu kako bi se utvrdila moguća prijevara (npr. da je testu pristupio netko drugi). Na primjer, ako se utvrdi da pristupnik testu živi u jednoj državi, a često i u kratkom vremenskom razdoblju pristupa testovima u drugim državama može se posumnjati da netko drugi pristupa testu ili da se radi o organiziranom varanju.

j. U situacijama kada se testiranje organizira u redovitim terminima, moguće je pratiti vrijeme početka i kraja testiranja kako bi se osiguralo da je testiranje organizirano u redovitom terminu. Organizacija testiranja izvan uobičajenog termina može upućivati na pokušaj varanja ili krađe sadržaja testa.

21. Računalne programe za razvoj testova, primjenu ispita ili upravljanje programom treba razvijati korištenjem sigurnosnih procedura koje štite od uobičajenih računalnih nestabilnosti i koje je potrebno povremeno provjeravati (npr. simulacijama napada drugih osoba).

22. Korigiranje računalno primijenjenih testova obično se provodi odmah nakon testiranja, a može se organizirati i tijekom testiranja nakon odgovora na svako pitanje (npr. računalno prilagodljivo testiranje). Prijetnje i rizici varanja tijekom ovog procesa korigiranja su minimalni. Za testove tipa papir-olovka korigiranje traje duže i uključuje više koraka te je potrebno primijeniti više sigurnosnih mjera kako bi se osiguralo da ne dođe do manipulacije rezultatima.

    a. Moguće je pripremiti neslužbene rezultate koje treba potvrditi nakon utvrđivanja njihove valjanosti. To može uključivati propise koji određuju da se rezultati ne smiju objaviti ili proglasiti službenima dok se ne pregledaju izvještaji o neregularnostima te dok se ne dovrše i pregledaju forenzične analize.

    b. Korigiranje računalnih oblika testova treba se provesti na zaštićenim udaljenim serverima, a ne na računalu pristupnika. Kod testova papir-olovka, može doći

do manipulacija listovima za odgovore nakon što se ovi prikupe i vrate na lokaciju za skeniranje ili čuvanje. Potrebno je osigurati proces praćenja kojim će se pažljivo nadgledati i zaštititi papirnate oblike listove za odgovore prije obrade za potrebe korigiranja.

23. Testovi, čestice, rezultati testiranja i druge važne informacije (npr. demografske informacije o pristupnicima) često se, bez obzira na to radi li se o papir-olovka ili digitalnim testovima, čuvaju dugo vremena nakon testiranja (npr. moguće i više godina). Bez obzira na to gdje i kada se ti podaci daju i prikupljaju, treba definirati profesionalne postupke koji će osigurati da neprikladan pristup tim informacijama (npr. hakiranjem) bude iznimno težak te da prikupljene rezultate i druge podatke nije moguće pronaći, promijeniti ili izbrisati bez prave autorizacije. Potrebno je redovito provjeravati i nadograđivati IKT procedure i sustave.
24. Prije, tijekom i nakon vremenskog okvira[4] primjene testa, program treba započeti proces praćenja interneta kojim će potražiti dokaze o otkrivanju sadržaja testa. Primjeri takvog otkrivanja mogu uključivati neobavezne rasprave o testu ili nekim pitanjima među pristupnicima, ili točnu reprodukciju jednog ili više testnih pitanja. Kada se to otkrije, program treba poslati prikladni zahtjev osobi zaduženoj za održavanje stranice i zatražiti prestanak rasprave, upozoriti sudionike i ukloniti sadržaj. Ako se materijal brzo ne ukloni, treba razmotriti strože postupke, uključujući pravne tužbe.
25. Prije, tijekom i nakon primjene testa, program treba zaštiti sadržaj testa i spriječiti njegovo izlaganje osobama koje nisu ovlašteni pristupnici testu ili predstavnici programa za testiranje koji ima pravo vidjeti sadržaj.

3. dio: Odgovor na povredu sigurnosti

Izvor prijetnje ponekad uspije probiti obranu programa, što rezultira uspješnim varanjem ili krađom sadržaja testa. Sljedeće smjernice nude savjete i podršku u rješavanju takvih situacija. Kada se otkrije prijevara ili krađa testa ili testnih čestica, program za testiranje tu povredu treba dubinski istražiti, zaustaviti, popraviti štetu i napraviti druge prikladne radnje. Potrebno je poduzeti korake koji će spriječiti buduće povrede sigurnosti.

Odbor za sigurnost trebao bi biti potpuno odgovoran za odgovor na povredu sigurnosti i imati pravo donositi odluke. Program će saznati za moguće ili stvarne povrede na različite načine, od kojih su neki bolji i lakši od drugih. Ovo su neki od njih:

- od novinara ili iz drugih medija
- iz prokuratorova izvještaja o neregularnostima
- iz dojave

4 Vremenski period u kojem je moguće primijeniti test.

- iz forenzičnog izvještaja o podacima
- iz izvještaja o praćenju mreže (interneta)
- od automatiziranih „sustava" sigurnosti (npr. korištenja neprikladnih pokreta na tipkovnici tijekom testiranja; pokušaja hakiranja)

Bez obzira na izvor povrede, program za testiranje treba brzo djelovati kako bi se odredila valjanost izvješća i opseg povrede. S tim informacijama moguće je poduzeti prikladne akcije. Tijekom testiranja, sustav za praćenje ili primjenu treba poduzeti akcije odmah čim se povreda dogodi. Prije i nakon testiranja, odbor za sigurnost odgovoran je za procjenu detalja povrede i prikladnu reakciju.

Specifične smjernice za odgovaranje na povredu sigurnosti

1. Testiranje pristupnika treba privremeno ili trajno zaustaviti ako prokuratori (na licu mjesta ili na mreži) ili osobe koje primjenjuju test primijete varanje. Pristupniku treba ponuditi objašnjenje.
   a. Nakon ispitivanja pristupnika koji je osumnjičen ili optužen za varanje ili zanemarivanje pravila testiranja, prokurator ili osoba koja provodi testiranje može dopustiti nastavak testiranja ili odlučiti da treba nastaviti pauzu ili otkazati test.
   b. Svaki neprikladni materijal treba zaplijeniti ako to dopuštaju relevantni zakoni. Pristupniku testiranja treba objasniti zašto je to nužno.
   c. Prokurator, nadzornik ili osoba koja provodi testiranje treba ispuniti izvještaj o neregularnosti testiranja i proslijediti ga odboru za sigurnost procesa testiranja.
   d. Ako se dopusti nastavak testiranja, odbor za sigurnost treba pripremiti i pregledati izvještaj o neregularnosti.
2. Povredu treba detaljno istražiti kako bi se ustanovila njezina ozbiljnost i opseg štete. Istraživanje može uključivati intervjue s osobama osumnjičenima za uključenost ili svjedoke, forenzičnu analizu podataka s ciljem određivanja učinaka na rezultate i/ili praćenje aktivnosti na mreži kako bi se odredila količina otkrivenog sadržaja.
3. Kompromitirani test ili skup čestica treba što prije zamijeniti.
   a. Unutar nekih programa za testiranje može se razmotriti korištenje ranije pripremljenog testa, tzv. formata testa za primjenu nakon povrede, kao zamjene za ukradeni test ili skup čestica.
4. Rezultate za koje se utvrdi da zbog prijevare nisu točni treba poništiti.
   a. Ovaj proces moguće je pojednostavniti ako se definiraju propisi koji određuju rutinsku provjeru rezultata koji se smatraju nepotvrđenima dok ne stigne potvrda.
   b. Ako je nevaljani testni rezultat već poslan pristupnicima, njih je potrebno odmah kontaktirati i informirati da im rezultati više nisu valjani te da će se sve odluke utemeljene na njima ponovno razmotriti.

5. Ako to povećava točnost rezultata potrebnih za donošenje odluke (npr. nakon pronalaska i uklanjanja kompromitiranih čestica), može biti poželjno ponovno korigirati/bodovati kompromitirani test.
6. Ovisno o propisima testnog programa i količini štete nakon povrede, moguće je provesti dodatne akcije koje mogu uključivati prekršajne ili kaznene prijave.
7. Treba kontaktirati mrežne stranice koje bez dopuštenja prodaju zaštićene čestice i zatražiti da se sadržaj ukloni sa stranice i svih drugih lokacija. Moguće je poduzeti još neke ozbiljnije korake. Mrežnu stranicu treba pažljivo motriti kako bi se provjerilo je li sadržaj uklonjen.
   a. Djelatnici programa mogu poslati dopise urednicima mrežne stranice kojima ih obavještavaju o problemu i traže uklanjanje materijala. Do sada se to pokazalo kao učinkovit prvi korak nakon kojeg većina urednika odgovori brzo i pozitivno.
   b. Ako materijal ostane na stranici, moguće je poslati formalnije pismo kojim se traži uklanjanje sadržaja pod prijetnjom pravne tužbe. Te obavijesti mogu se referirati na relevantne državne ili regionalne zakone (npr. *Digital Millennium Copyright Act* u SAD-u ili europski propis *Copyright Directive*).[5]
8. Ovisno o propisima i ozbiljnosti povrede, moguće je tražiti i dopustiti da pristupnici ponovo pristupe testiranju u kojem se može koristiti ista ili druga forma testa. Ako je to u skladu s važećim zakonima, moguće je ograničiti pristup osobama koje su uključene u varanje ili krađu testova.
   a. Propisi trebaju jasno definirati pravila za ponovno testiranje oko kojih se trebaju dogovoriti svi sudionici, uključujući pristupnike testa, prije primjene testa.
   b. Ako je moguće, prilikom ponovnog testiranja treba koristiti novu formu testa.
   c. Dodatni uvjeti (npr. novčana kazna ili privremena zabrana) mogu se primijeniti kao uvjeti za ponovno testiranje.
9. Nakon povrede, moguće je očekivati povećani interes sudionika i drugih osoba (npr. medija) i/ili javnosti. Važno je što brže razviti i distribuirati dokumente za učinkovitu komunikaciju. Zapošljavanje agencije za odnose s javnostima ili glasnogovornika također može pomoći. Pripremljeni materijali mogu uključivati standardizirane obavijesti o povredi sigurnosti, ozbiljnosti te povrede i postupcima kojima se pokušava odgovoriti na nju.

5 U Republici Hrvatskoj su na snazi propisi koji uređuju autorsko i izdavačko pravo: Zakon o autorskom pravu i srodnim pravima (NN 167/03; 79/07; 80/11; 125/11; 141/13; 127/14), Zakon o psihološkoj djelatnosti (NN 47/03), Pravilnik o psihodijagnostičkim sredstvima Hrvatske psihološke komore, te Kazneni zakon (NN 144/12), koji na određeni način sudjeluje u jamstvu ostvarivanja i razvoja intelektualnog vlasništva inkriminirajući nedopuštena ponašanja kojima se krše ta prava, između kojih je najznačajnije i najčešće neovlašteno reproduciranje, prerađivanje, umnožavanje itd. (nap. prev.)

10. Nakon povrede, može biti potrebno provesti procjenu trenutačnog sigurnosnog plana i povezanih procedura kako bi se odredilo je li potrebno mijenjati ili dodavati sigurnosne propise ili procedure. Ako je potrebno donijeti takve promjene, s njima treba upoznati sve sudionike te pripremiti i odobriti novi sigurnosni plan.

POJMOVI I DEFINICIJE

Analiza latencije (eng. Latency Analysis). Oblik forenzične obrade latencije odgovora, odnosno vremena reakcije od trenutka prezentacije čestice do trenutka u kojem pristupnik odgovori na pitanje i pošalje svoj odgovor. Neuobičajeno kratke ili duge latencije mogu upućivati na varanje ili na neki drugi sigurnosni problem.

Analiza rizika (eng. Risk Analysis). Analiza različitih sigurnosnih prijetnji programu za testiranje s ciljem procjene vjerojatnosti rizika, moguće štete i prikladnog raspoređivanja sredstava za obranu sigurnosti.

Autentifikacija (eng. Authentication). Proces kojim se potvrđuje da osoba koja je pristupila ili se priprema pristupiti testiranju zaista jest osoba koja treba pristupiti testiranju. Autentifikacija nije jednaka identifikaciji, kod koje se pokušava odrediti identitet pristupnika.

Banke čestica (eng. Item Pools). Veće baze čestica iz kojih se prije ili tijekom testiranja biraju pojedinačna pitanja od kojih je sastavljen test.

Biometrijske metode (eng. Biometrics). Metode prikupljanja jedinstvenih informacija o pristupnicima koje se mogu koristiti u procesu autentifikacije ili identifikacije.

Čestice „trojanski konji“ (eng. Trojan Horse Items). Čestice u ispitu kod kojih su odgovori namjerno promijenjeni. Ovim česticama pokušava se otkriti ispitanik koji pokušava varati na testu korištenjem ukradenih čestica i lista za odgovore.

Dinamika korištenja tipkovnice (eng. Keystroke Dynamics). Biometrijska metoda kod koje se uspoređuju obrasci tipkanja ispitanika u trenutku registracije i neposredno prije početka testa.

Forenzična obrada (eng. Data Forensics). Metode kojima se analiziraju testni rezultati s ciljem pronalaska obrazaca koji mogu upućivati na varanje ili krađu testa.

Forma testa za primjenu nakon povrede (eng. Breach Test Form). Alternativna forma testa koja zamjenjuje kompromitiranu formu.

Identifikacija (eng. Identification). Proces identificiranja osobe koja pristupa testiranju ili se na to priprema. Identifikacija nije isto što i autentifikacija, prilikom koje se ne pokušava identificirati ispitanika.

Ispitanik (eng. Examinee). Osoba koja pristupa testu. Naziva se i pristupnik testiranju.

Istraga (eng. Investigation). Proces određivanja uzroka i opsega povrede. Istrage mogu uključivati intervjue, forenzičnu obradu, analizu procedura, pregled izvještaja itd.

Izloženost čestice (eng. Item Exposure). Pokazivanje čestice tijekom testiranja pojedinim ispitanicima, ili izloženost čestice nakon što je nelegalno ukradena i distribuirana putem interneta ili na neki drugi način.

Izvješća o neregularnostima (eng. Irregularity Reports). Izvješća koja pripremaju prokuratori i druge osobe, a u kojima se opisuje varanje ili drugi neuobičajeni činitelji koji su utjecali na primjenu testa.

Kompromitiranost čestica i testa (eng. Compromise of Items and Tests). Nalaz da je sadržaj testa bio neprikladno izložen i da možda više nije prikladan za korištenje.

Krađa testa (eng. Test Theft). Bilo koje ponašanje kojim se pokušava ili uspijeva nelegalno preuzeti sadržaj testa.

Manipulacija listovima za odgovore (eng. Tampering with Answer Sheets). Oblik varanja kod kojeg se netočni odgovori na listu za odgovore brišu i zamjenjuju točnima.

Nadzornik (eng. Invigilator). Osoba odgovorna za sigurnost testa tijekom njegove primjene. Naziva se i prokurator.

Neslužbeni rezultati (eng. Provisional Scores). Neslužbeni rezultati koji se prezentiraju ispitanicima nakon završetka ispita i koje treba pregledati odbor za sigurnost.

Obrisani odgovori (eng. Erasures). Odgovori na listu za odgovore koji su bili izbrisani.

Organizirano varanje (eng. Collusion). Niz osoba koje zajednički rade s ciljem varanja na testu ili krađe sadržaja testa.

Pauza (eng. Break). Vrijeme za odmor između dijelova vremenski dužih ispita.

Ponovljeno testiranje (eng. Re-testing). Dopuštanje pojedincima da ponovno pristupe testiranju.

Ponovni izlazak na test (eng. Retakes). Ponovljeni pristup testiranju.

Ponovno korigiranje/bodovanje (eng. Rescoring). Proces ponovnog korigiranja/bodovanja testa koji se može provesti nakon uklanjanja utjecaja kompromitiranih čestica.

Poučavanje (eng. Coaching). Oblik organizirane prijevare kod koje jedan pojedinac pomaže drugom da odgovori na testna pitanja tijekom testiranja.

Povećanje rezultata (eng. Score Gains). Oblik forenzične obrade podataka kojim se analiziraju povećanja (ili smanjenja) rezultata s ciljem utvrđivanja neuobičajenih promjena koje bi mogle upućivati na varanje.

Povreda (eng. Breach). Uspješan napad od strane poznatih ili nepoznatih prijetnji.

Praćenje mreže (eng. Web Monitoring). Skup metoda za pretraživanje interneta s ciljem pronalaska korištenih testnih pitanja.

Prepoznavanje lica (eng. Facial Recognition). Biometrijska metoda kojom se putem računalne kamere uspoređuju crte lica ispitanika u trenutku registracije u program i prije početka testiranja.

Prezentacija čestica pitanje-po-pitanje (eng. Forward-Only Item Presentation). Čestice se u testu prikazuju bez mogućnosti vraćanja na prethodno prezentirane čestice.

Prijetnja (eng. Threat). Osoba ili metoda koja može uspješno varati na procjeni ili uspješno ukrasti sadržaj testa.

Pristupnik (eng. Test Taker). Osoba koja pristupa testiranju. Naziva se također ispitanik.

Procjena s visokim ulozima (procjena velike važnosti) (eng. High-Stakes Assessments). Testovi i drugi oblici procjena čiji rezultati imaju značajne posljedice za pojedinca ili organizaciju.

Prokurator (eng. Proctor). Osoba odgovorna za sigurnost testa tijekom njegove primjene. Naziva se i nadzornik.

Provjere životopisa (eng. Background Checks). Proces provjere životopisa osobe s ciljem utvrđivanja je li ta osoba kvalificirana za pomaganje u konstrukciji ispita.

Različite metrijske karakteristike čestica (eng. Differential Item Performance). Oblik usporedbe čestica unutar forenzične obrade u različitim uvjetima (npr. nakon završetka testiranja i nakon šest mjeseci) koji može pokazati kompromitiranost čestice.

Rizik (eng. Risk). Procjena vjerojatnosti da prijetnja postane uspješna povreda i opsega štete koju bi takva povreda mogla prouzročiti.

Sigurnosni plan (eng. Security Plan). Dokument u kojem su opisani sigurnosni procesi i procedure neke organizacije.

Slabost (eng. Vulnerability). Slabost u obrani sigurnosti programa.

Sličnost odgovora (eng. Similarity of Responses). Oblik forenzične obrade podataka kojim se uspoređuju profili odgovora dvaju ili više pojedinaca kako bi se odredilo jesu li bili u dosluhu, je li došlo do zamjene pristupnika testiranju ili poučavanja.

Test za provjeru (verifikacijski test) (eng. Verification Test). Test koji se naknadno primjenjuje s ciljem provjere izvedbe ispitanika na prethodnom testu.

Testna pomagala (eng. Test Aids). Uređaji ili dokumenti koje ispitanik može koristiti tijekom testiranja. Treba napomenuti da neka od tih pomagala (npr. kalkulatori) mogu biti dopuštena.

Ubačene čestice (eng. Embedded Items). Proces namjernog ubacivanja čestica koje se u testu ne boduju kako bi se identificirali pojedinci koji varaju korištenjem ranije prikupljenih informacija o testu.

Varanje (eng. Cheating). Bilo koje ponašanje kojim se pokušava ili uspijeva na neprikladan način povećati testni rezultat.

Zaključavanje (eng. Lockdown). Program koji se pokreće prije početka samog testa primijenjenog putem interneta, a koji ispitaniku ograničava korištenje tipkovnice i računalnih funkcija samo na one koje mu omogućuju prolazak kroz test i odgovaranje na pitanja. Pristup drugim resursima, primjerice tvrdom disku računala, internetu i nekim kombinacijama tipki je zabranjen.

Zamjenik pristupnika testu (eng. Proxy Test Taker). Osoba koja umjesto nekog drugog pristupa testu.

Žetva čestica (eng. Item Harvesting). Uspješni ili neuspješni pokušaji nelegalnog bilježenja sadržaja testa kojima se krše sigurnosna pravila programa.

LITERATURA

Foster, D. F., Miller, H. L., Jr. (2012). Global Test Security Issues and Ethical Challenges. U: A. Ferrero, Y. Korkut, M. M. Leach, G. Lindsay, M. J. Stevens (Ur.). *The Oxford Handbook of International Psychological Ethics* (str. 216-232). Oxford: Oxford University Press.

Prevela: doc. dr. sc. Andreja Bubić

[Bilješke]

[Bilješke]