razultat toga razvili su se standardi i okviri koji danas čine podlogu za uspješno upravljanje informacijskom sigurnošću i informacijskim sustavima.

Sukladno s Politikom i Smjernicama za izradu metodologije procjene rizika preporučuje se Institucijama BiH da donesu svoje interne akte sukladno koracima definiranim u dijagramu procjene rizika.

LITERATURA:

1. Politika upravljanja informacijskom sigurnošću u institucijama Bosne i Hercegovine za period 2017. -2022. godina ("Službeni glasnik BiH " broj 38/17)
2. Standard ISO/IEC 27001 - Sigurnosne tehnike - sustavi za upravljanje sigurnošću informacija - Zahtjevi Standard ISO/IEC 27002
3. Stoneburner, G., Goguen, A., Feringa, A.(2002.) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce: NIST [online].NIST SP 800-30.

На основу члана 17. Закона о Савјету министара Босне и Херцеговине ("Службени гласник БиХ", бр. 30/03, 42/03, 81/06, 76/07, 81/07, 94/07 и 24/08) и Поглавља 3. Одлуке о усвајању Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине за период од 2017 - 2022. године ("Службени гласник БиХ", број 38/17), на приједлог Министарства комуникација и транспорта Босне и Херцеговине, Савјет министара Босне и Херцеговине на 54. сједници, одржаној 28. јула 2022. године, донио је

ОДЛУКУ
О УСВАЈАЊУ СМЈЕРНИЦА ИЗ ПОЛИТИКЕ УПРАВЉАЊА ИНФОРМАЦИОНОМ БЕЗБЈЕДНОШЋУ У ИНСТИТУЦИЈАМА БОСНЕ И ХЕРЦЕГОВИНЕ ЗА ПЕРИОД ОД 2017 - 2022. ГОДИНЕ

Члан 1.

(Предмет Одлуке)

(1) Овом одлуком усвајају се смјернице из Политике управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017-2022. године, и то:
   а) Смјернице о корисничким рачунима и правима приступа,
   б) Смјернице о безбједносним копијама,
   ц) Смјернице о запослењу и прекиду запослења и
   д) Смјернице за израду методологије и процјене ризика.

(2) Смјернице из става (1) овог члана су прилози ове одлуке и чине њен дио.

Члан 2.

(Праћење реализације Одлуке)

За праћење реализовања ове одлуке задужују се Министарство комуникација и транспорта Босне и Херцеговине и Министарство безбједности Босне и Херцеговине.

Члан 3.

(Ступање на снагу)

Ова одлука ступа на снагу даном доношења и објављује се у "Службеном гласнику БиХ".

СМ број 93/22
28. јула 2022. године
Сарајево

Предсједавајући
Савјета министара БиХ
Др **Зоран Тегелтија**, с. р.

СМЈЕРНИЦЕ
О КОРИСНИЧКИМ РАЧУНИМА И ПРАВИМА ПРИСТУПА

1. Сврха

Сврха документа је обезбједити контролу над отварањем, измјеном, замрзавањем и затварањем корисничких рачуна у информационом систему, у циљу спрјечавања застарјелих, редундантних и корисничких рачуна отворених на неисправан начин. Право приступа вриједностима информационог система једна је од најкритичнијих тачака безбједности. Због наизглед компликованог процеса додјељивања права приступа, корисницима се често додјељују "уобичајена" права, која су најчешће пуно већа од потребних. Што већа права приступа корисник посједује, веће су могућности да случајним или намјерним радњама угрози безбједност информационог система.

Обављање основне дјелатности институције повезано је са руковањем подацима који се налазе у информационом систему. Због тога је неопходно да запосленима буде омогућен приступ различитим подацима у оквиру система. Међутим, приступ запослених овим подацима треба да буде усаглашен са процесном структуром организационог система. Запосленима је потребно обезбједити приступ само оним подацима и дијеловима информационог система који су им потребни за реализацију активности за које су надлежни, а не комплетном информационом систему. Из тог разлога потребно је прилагодити права приступа информационом систему описима послова из важећег правилникао о унутрашњој организацији и систематизацији радних мјеста. Такође, уколико је институција имплементирала систем управљања квалитетом, потребно је усагласити права приступа запослених са њиховим улогама у процедурама.

Неопходно је обезбједити да је приступ информационом систему омогућен само онима који за то имају правни основ, уз одговарајућу евиденцију сваког приступа и евентуалног ажурирања. Због тога је неопходно имплементирати систем корисничких улога (рола), којим ће бити дефинисани одговарајући нивои права приступа прикупљеним подацима у информационом систему. Систем улога мора прецизно да дефинише најпре којим подацима корисник коме је додељена одређена улога уопште може да приступи, а затим и на који све начин може да их обрађује. Институција треба да успостави механизам креирања и укидања корисничких налога, те да води евиденцију свих корисничких налога у оквиру информационог система, како активним, тако и укинутим налозима. Институција прописује процедуре додјеле и укидања налога, те провјере адекватног нивоа приступа и додјеле јединствене идентификационе ознаке сваког налога.

2. Приступ информационом систему

Приступ информационом систему се базира на подацима за аутентификацију, као што су лозинке, криптографски кључеви, токени, смарт картице, пин код и 2ФА апликације. Дистрибуцију и чување ових података регулише институција, како би се спријечиле безбједносне пријетње попут откривања података за аутентификацију запослених (колегама, породици или трећим лицима) или записивање шифре у нотесу или на наљепници.

Основно правило при креирању лозинке јесте избјегавање података из приватног живота као што су датум рођења, име кућног љубимца, омиљено мјесто и слично, као и било какве ријечи природног језика. Класичне методе пробијања лозинке данас подразумијевају аутоматизоване претраге по списковима ријечи (dictionary attack), а који могу обухватати на милионе појмова из различитих језика. Шифра од 12 бро-

јева има 1.000.000.000.000 комбинација, прецизније 10^12, шифра од 12 знакова која садржи цифре, велика и мала слова и специјалне карактере има 475.920.310.000.000.000.000.000 комбинација, имајући у виду да је укупан број свих алфанумеричких и специјалних карактера 94. Шифра од 12 бројева или мање, може се разбити за мање од сат времена. Са технологијом у слободној продаји, потребно је око пет милиона година да би се пробила шифра исте дужине која, осим бројева, садржи велика и мала слова и специјалне карактере. Код информационих система предвиђених за велики број корисника, администратори уобичајено аутоматски генеришу иницијалне лозинке. Неријетко, лозинке се корисницима шаљу електронском поштом, што није безбједан канал комуникације. Да би се елиминисао ризик од пресретања поруке која садржи лозинке, не треба их слати електронском поштом. Приликом развоја информационих система, систем треба поставити тако да администратор креира налоге само са корисничким именима, а да се корисницима препусти могућност да сами поставе лозинку приликом прве пријаве у систем, користећи адекватан дигитални цертификат или токен како би потврдили свој идентитет. Све лозинке се чувају у базама или датотекама које се налазе на серверима. Такве базе се морају енкриптовати, тако да ни сам систем администратор не може да их прочита. Из практичних разлога администратору треба оставити могућност да ресетује лозинке.

Јак систем аутентификације подразумјева више од једног захтјева приликом приступа - не само корисничку лозинку, већ и квалификовани сертификат. Двострука провјера подразумјева захтјев за потврду идентитета лозинком и цертификатом. Предност коришћења оваквог система налази се у додатној препреци, у случају да је лозинка украдена. Поред информационих система, двоструку провјеру би требало користити и за остале налоге запослених (електронска пошта, налози на друштвеним мрежама, финансијске апликације и слично). Дигитални цертификати се могу примјенити на више начина, али је најједноставније дистрибуирати их у облику смарт картица или УСБ токена. Уколико се користе цертификати у облику картица, за њихову употребу неопходни су одговарајући читачи, док се УСБ токени користе преко постојећег УСБ улаза на рачунару.

Лог је регистар свих догађаја у оквиру једног система, односно свих активности корисника - од пријаве, преко уноса података до њихових промјена, штампања, брисања и других поступака. Логови могу биљажити активности у различитим дијеловима система. Основни облик је приступни лог (access log), а његову структуру, као и структуру свих логова, подешава администратор информационог система. Приликом подешавања треба имати на уму да лог треба да буде довољно детаљан да омогући јасно утврђивање злоупотреба (неовлашћени приступи и друге активности) али да не буде превише комплексан за анализу или складиштење. Сваки приступни лог би требало да садржи конкретне информације:

- корисник који је приступио бази података;
- датум и вријеме приступа;
- ИП адреса са које је приступљено бази података;
- ресурс коме је приступљено;
- врста обраде података (преглед/унос/измјена/брисање/извоз/штампа).

Логове је потребно чувати најмање годину дана, а уколико постоји могућност и дуже. Поред тога, информациони систем је неопходно пројектовати тако да се за сваки његов сегмент (апликације, подаци, остали ресурси) од тренутка настанка, па све до тренутка брисања, памте све измјене. Дакле, приликом сваке измјене потребно је чувати конкретне информације:

- корисник који је извршио измјену;
- врста измјене (унос, измјена, брисање података, надоградња софтвера, инсталирање нових апликација итд);
- датум и вријеме измјене;
- вриједност податка прије измјене.

Институција треба да надгледа развојни процес како би имала сазнања о томе да ли се наложени стандарди имплементирају у систем. Како би то било могуће, институција, заједно са трећим лицем које развија информациони систем, треба да документује, систематизује и квантификује све врсте безбједносних захтјева и стандарда које информациони систем треба да садржи, још прије почетка пројектовања. Касније, током напреднијих фаза развоја, имплементацију ових стандарда такође треба документовати.

Додјела права приступа:

- сваки корисник приликом отварања корисничког рачуна, зависно којој групи корисника припада, има минимална, тзв. **основна** права,
- сваком кориснику могуће је проширити основна права уколико за тим постоји потреба,
- додатна права приступа може додијелити одговорна особа (запосленик институције који има право додјеле права приступа),
- за право приступа осјетљивим и тајним подацима, корисник је дужан потписати изјаву о придржавању правила безбједности дефинисаних Политиком управљања информационом безбједношћу у институцијама БиХ за период 2017.-2022. године,
- право приступа трећој страни додјељује одговорна особа; прије додјељивања права приступа трећа страна је дужна потписати изјаву о придржавању правила безбједности дефинисаних Политиком управљања информационом безбједношћу у институцијама БиХ за период 2017.-2022. године,
- уколико трећа страна захтјева приступ осјетљивим или тајним подацима, потребна је сагласност руководиоца институције,
- сва додијељена права приступа морају бити јасно документована,
- потребно је омогућити увид у која права приступа има поједини корисник или група корисника,
- потребно је омогућити увид ко све има права над појединим ресурсом, с могућношћу филтрирања резултата.

3. Евиденција захтјева

Правовремено затварање корисничког рачуна важна је карика у безбједности информационих система. Уколико "неважећи" кориснички рачун није затворен, кориснику је отворен пут обављању злонамјерних радњи. Како би процес отварања и затварања корисничких рачуна био правовремено и квалитетно обављен, потребно је дефинисати начине комуникације између подносиоца захтјева и администратора система, те начин евиденције захтјева за отварањем односно затварањем рачуна. Приједлог комуникације и евиденције захтјева:

- комуникација са особом одговорном за управљање корисничким рачунима обавља се унапријед дефинисаним протоколом, нпр. путем web апликације,
- како би подносилац захтјева приступио апликацији, потребно је обавити провјеру аутентичности и ауторизацију,
- подносилац захтјева на свом рачунару отвара апликацију и задаје захтјев за отварањем/затварањем корисничког рачуна,

- захтјев се похрањује у базу података,
- администратор има могућност прегледа захтјева према критерију,
- администратор је дужан редовно прегледавати захтјеве,
- затварање захтјева има предност над отварањем захтјева.

Протокол комуникације између подносиоца захтјева и одговорне особе, те евиденције самих захтјева може бити реализован и на неки други начин одобрен од стране институције.

4. Отварање корисничког рачуна

Кориснички рачун могуће је отворити:
- запосленима,
- трећој страни.

Процедура отварања корисничког рачуна:

запосленима:
- овлашћена особа институције путем апликације подноси захтјев за отварање корисничког рачуна новом запосленом,
- администратор система на основу добијених података отвара кориснички рачун.

трећој страни:
- за отварање корисничког рачуна трећој страни потребна је сагласност овлашћеног лица (администратор информационог система) институције,
- овлашћено лице је главно и одговорно лице у сарадњи са трећом страном, и као такво има права давања сагласности за отварање корисничких рачуна,
- код отварања корисничког рачуна за трећу страну потребно је одредити временски период колико ће рачун бити активан.

5. Замрзавање корисничког рачуна

У случају дужег планираног некоришћења информационог система (нпр. због едукације у иностранству, болести, неплаћено одсуство и сл.) кориснички рачун потребно је замрзнути (преко Active Directory за институције које су кориснице еВладе). Замрзавањем корисничког рачуна избјегавају се непотребни поступци затварања и отварања рачуна, али и спрјечавају безбједносни инциденти који могу настати коришћењем корисничког рачуна од стране других лица док стварни власник није присутан. Замрзавање рачуна одвија се на начин да подаци остану у бази података о кориснику, али се у посебно поље назначи да је рачун замрзнут. Замрзнутом корисничком рачуну није потребно мијењати лозинку у одређеном временском периоду како је дефинисано политиком. Такође се заобилазе све друге безбједносне контроле од стране система за које је потребна интеракција корисника. Замрзнути кориснички рачун могуће је вратити у употребу (одмрзнути) на захтјев корисника и одговорне особе, с тиме да захтјев мора бити документован и одобрен као и код отварања новог захтјева.

6. Затварање корисничког рачуна

Затварање корисничког рачуна посебно је осјетљив поступак, а осјетљивост зависи о организацији управљања корисничким рачунима. Што је управљање рачунима неквалитетније изведено, то ће затварање корисничких рачуна бити компликованије. На примјер, ако се кориснички рачуни отварају без документовања и на основу тренутних потреба, након нпр. године дана више се не зна ко има право приступа над којим ресурсима. Тада је и затворити кориснички рачун пуно теже. Уколико "затвореном" кориснику остану нека права приступа, пут за почињење злонамјерних акција му је отворен. Ово је још један примјер зашто је квалитетна организација корисничких рачуна потребна.

Затварање корисничког рачуна одвија се кроз сљедеће фазе:
- при прекиду радног односа потребно је предати захтјев о затварању корисничког рачуна запосленог,
- трећим лицима кориснички рачун се затвара након дефинисаног временског периода приликом отварања рачуна, или уколико је потребно прије на захтјев одговорног лица задуженог за сарадњу са трећом страном,
- лице одговорно за вођење корисничких рачуна дужно је редовно прегледавати запримљене захтјеве за затварањем рачуна те их правовремено затворити,
- уколико постоји потреба, кориснику је могуће пријевремено затворити кориснички рачун без претходног обавјештења на основу писаног захтјева овлашћене особе институције.

7. ЗАКЉУЧАК

У складу са Политиком и Смјерницама о корисничким рачунима и правима приступа препоручује се Институцијама БиХ да донесу свој интерни акт у којем ће дефинисати **правила/процедуре о корисничким рачунима и правима приступа**.

Литература

1. Политика управљања информационом безбједношћу у институцијама Босне и Херцеговине за период 2017. – 2022. година ("Службени гласник БиХ", број 38/17)
2. Стандард ИСО/ИЕЦ 27001 – Безбједносне технике – Систем за управљање безбједношћу информацијама – Захтјеви
3. Стандард ИСО/ИЕЦ 27002 – Безбједносне технике – Правило добре праксе за контроле безбједности информација
4. Закон о заштити тајних података ("Службени гласник БиХ", број 54/05 и 12/09)

СМЈЕРНИЦЕ О БЕЗБЈЕДНОСНИМ КОПИЈАМА

1. Сврха

Данас рачунари и апликације служе за повећавање продуктивности, смањивање трошкова и уштеду времена потребног за обављање посла. Уколико се недовољна пажња посвети ризицима који угрожавају рачунарске системе, у институцијама су могуће ситуације које могу узроковати застоје у пословању. Да се не би догодио непланирани застој, институције морају редовно извршавати процедуре за израду и одржавање резервних копија. У противном може доћи до катастрофалних посљедица. Узрок томе је што је пословање зависно у информационим технологијама. Пред информатичке податке се постављају високи критерији заштите који су једнаки или чак већи од критерија заштите записа у пословним књигама. Информациони систем је дио инфраструктуре институције те је из тог разлога недоступност истог или уништење података велики ризик за који треба планирати мјере контроле и обављати поступке којима се повећава потпуно, безбједно и јефтино враћање података.

Израда резервних копија (енг. backup) је основна претпоставка која се поставља пред систем који мора задовољавати резервне захтјеве. Поступак израде резервних копија заједно са поступком повратка података, представља основну процедуру којом се систем штити од губитка података и обезбјеђује брза обнова података у случају