ДРЖАВЕН ЗАВОД ЗА РЕВИЗИЈА
ENTI SHTETËROR I REVIZIONIT
STATE AUDIT OFFICE

ДРЖАВЕН ЗАВОД ЗА РЕВИЗИЈА

- Соопштение за медиуми -

Скопје, 24.06.2024 година

Критичните информациски системи во ризик

Институциите и органите не обезбедуваат ефикасна и целосна заштита на критичните информациски системи заради отсуство на законска регулатива од областа на безбедноста на информациските системи, не усогласување со европските директиви и недоволната кадровска екипираност

Државниот завод за ревизија изврши ИТ ревизија како ревизија на успешност на тема **„Ефективност на преземените мерки на надлежните органи за заштита на критичните информациски системи“** согласно Годишната програма за работа на ДЗР за 2023 година.

Целта беше да се даде одговор на прашањето **„Дали преземените мерки од надлежните органи обезбедуваат ефикасна и целосна заштита на критичните информациски системи?“**

Со ревизијата се стекна разумно уверување дека **институциите и органите не обезбедуваат ефикасна и целосна заштита** на критичните информациски системи. Причини за ваквата состојба се недостаток на закони за безбедноста на информациските системи, неусогласеност со европските директиви, недостаток на стратешки документи, не функционирање на Националниот совет за сајбер безбедност и недоволна кадровска екипираност.

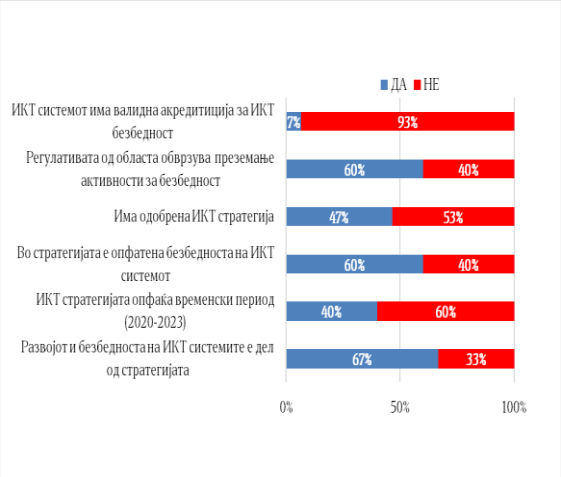
Во однос на законската регулатива и донесувањето на стратешките документи од областа на сајбер безбедноста со ревизијата констатирано е дека во 2019 година подготвен е предлог закон за безбедност на мрежи и информациски системи кој не е донесен, а во 2023 година подготвен е нов предлог закон кој се наоѓа во собраниска процедура.

Исто така, и незавршениот процес на меѓу институционално усогласување за Националната ИКТ стратегија, со важност до 2017 година и Националната

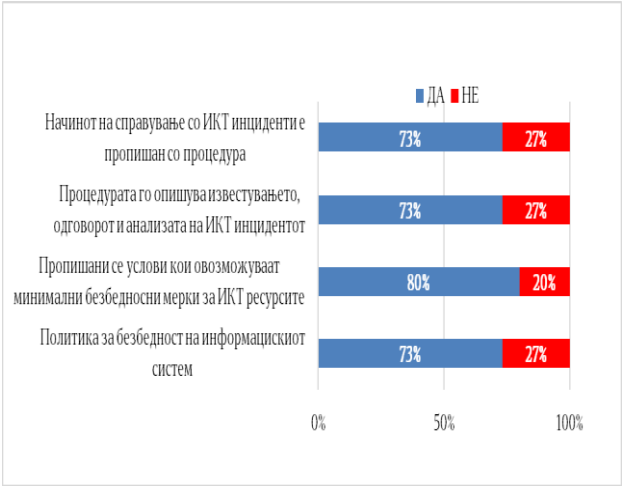
ул. Павел Шатев бр.2, Палата „Емануел Чучков“, 1000 Скопје, Република Северна Македонија
Pallata„Emanuel Çuçkov“, rr. Pavel Shatev nr.2, 1000 Shkup, Republika e Maqedonisë së Veriut
Pavel Shatev St 2, Palata Emanuel Cuckov, 1000 Skopje, Republic of North Macedonia
T: +38923211262 www.dzr.mk dzr@dzr.gov.mk

стратегија за сајбер безбедност, со важност до 2022 година, доведува до отсуство на стратешки документи како сет на активности и мерки, односно не обезбедува безбедна, еластична и доверлива дигитална средина која ќе влијае државата да биде безбедно место за он-лине делување и работа со напредни човечки и технички капацитети.

Со ревизијата извршена е анализа на одговорите за состојбата со ИТ управување во делот на стратешки документи како и мерки и стандарди за информациска безбедност, која покажа дека кај 53% од институциите кои го одговориле прашалникот не е одобрена ИКТ стратегијата, додека 40% воопшто ја немаат опфатено информациската безбедност во стратешките документи. Само една институција поседува сертификат за информациска безбедност, додека пак пропишаните документи за постапување и одговор по ИКТ инциденти отсуствуваат кај 27% од институциите



Стратешки документи за информациска безбедност



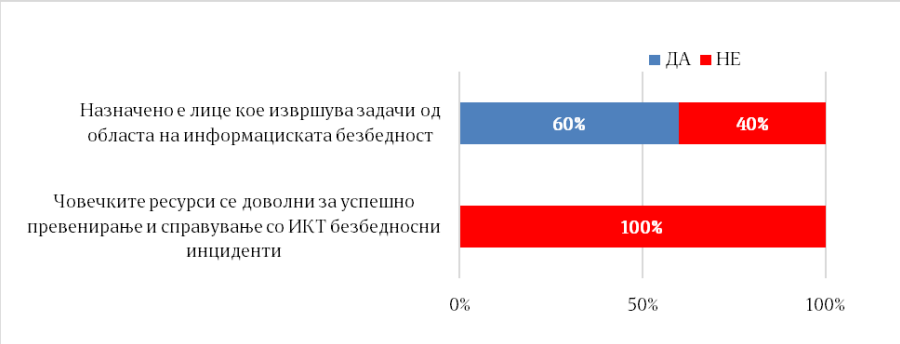
Пропишани мерки и стандарди за информациска безбедност

Утврдено е дека минималните безбедносни мерки и стандарди за заштита на информациските системи не се пропишани, истите не се усогласени со ЕУ директивите, што може да предизвика ризик од недоволни инвестиции и одложување на мерки за подобра заштита. Имено, Регистар на операторите на критична инфраструктура – Критична информациска инфраструктура (КИИ) и Важни информациски системи (ВИС) не е утврден поради отсуство на законски пропишана регулатива, а ваквата состојба оневозможува утврдување на инвестициите од областа на информациската безбедност и вкупна вредност на истите.

Од направената анализа на вредноста на склучените договори објавени во ЕСЈН на сите државни субјекти чиј предмет на набавка е од областа на информациската безбедност, не вклучувајќи ги инвестициите од оваа област спроведени преку

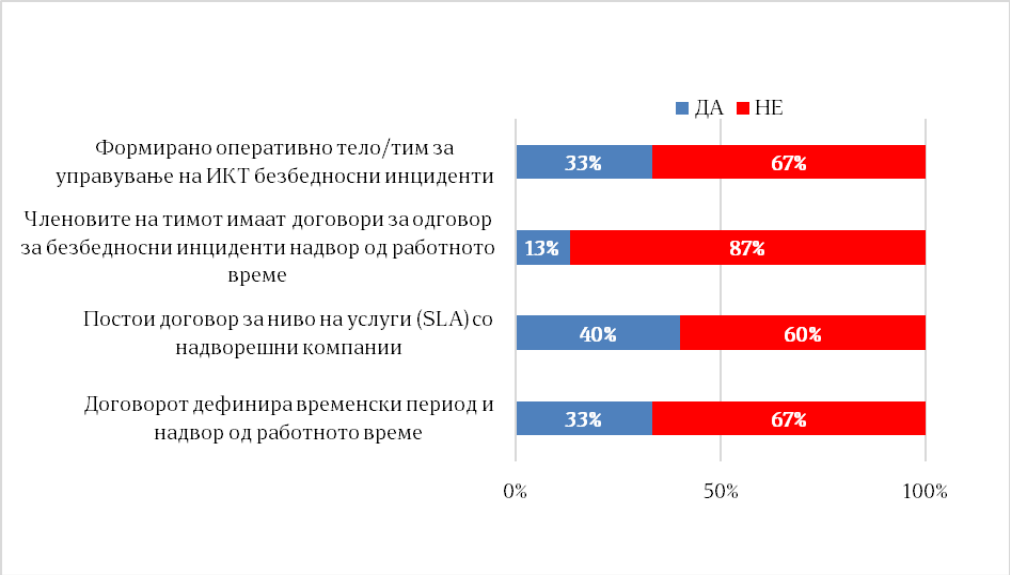
меѓународни проекти и грантови од институциите, ревизијата констатира дека за периодот 01.01.2020 до 15.12.2023 година, од склучени вкупно 69.504 договори во вкупна вредност од 205 милијарди денари (над 3 милијарди евра), од кои само за набавки чии предмет на набавка е од областа на информациската безбедност, склучени се 283 договори со 61 економски оператор во вкупна вредност од 377 милиони денари, што претставува 0,18% од вкупната вредност на склучените договори.
Од исклучителна важност е институциите финансирањето во информациската безбедност да го гледаат како инвестиција, а не како трошок при што ефектите се далеку поголеми во инвестирање на превентивни мерки од штета во однос на трошокот направен по безбедносен инцидент.

Кадровската екипираност за заштита на критични информациски системи, е на незавидно ниво. Од извршените анализи на добиените одговори од страна на сите институции, констатирано е дека кај сите институции недостасуваат човечки ресурси за превенирање и справување со ИКТ (Информациско комуникациска технологија) безбедносни инциденти, додека кај 40% од институциите воопшто не е назначено лице одговорно за информациска безбедност.



Во однос на оперативни тимови за справување на компјутерски безбедносни инциденти со ревизијата се утврди дека 67% од институциите немаат формирано тимови за одговор на компјутерски инциденти, додека кај 60% не се склучени договори со надворешни компании за пренесување на ризикот од безбедносен инцидент. Во однос на вработените ИТ лица во институциите, 87% воопшто немаат утврдено обврска за нивно ангажирање во случај на потреба надвор од работното

време, состојба која носи висок ризик од успешен одговор при соодветен сајбер напад или ИКТ безбедносен инцидент.



Во периодот опфатен со ревизијата до денот на известувањето констатирани се повеќе пропусти и непочитување на законските обврски и тоа:

- Не е пропишана пријавата на компјутерски безбедносен инцидент од страна на институциите до Националниот центар за одговор на компјутерски инциденти (МКД-ЦИРТ);
- Не е регулиран начинот на оневозможување пристап до интернет мрежата на инфицирани и малициозни уреди, приклучени преку интернет операторите;
- Отсуство на континуирана стручна обука за најновите закани по информацискатa безбедност;
- Неизвршена анализа на ризици како и предлог мерки според приоритет за нивно намалување, ублажување, пренесување или минимизирање на ризиците на прифатливо ниво, со точна временска рамка за спроведување на истите;
- Недостасува континуирана анализа за согледување на реалната состојба и дефинирање мерки за подигнување на нивото на безбедност, извршување на редовни ревизии за детектирање на грешки и ранливости на безбедноста, развој и периодично тестирање на планови на информацискатa безбедност во институциите, како и
- Потреба од дополнителни обуки за подигање на свесноста на вработените за ИКТ безбедност како и тестирање за проверка на свесноста меѓу другото и за препознавање на обидите за присвојување на идентитети.

Исто така, со ревизијата е констатирано дека Националниот совет за сајбер безбедност, формиран во 2019 година за спроведување на Националната стратегија за сајбер безбедност од 2018-2022, не функционира како што се очекуваше. Нефункционалноста на Советот ја доведува во прашање ефективноста, ефикасноста и релевантноста во справувањето со современите и идните

предизвици за сајбер безбедноста, улогата и способноста да функционира за време на сајбер-криза.

Со ревизијата дадени се препораки кои се однесуваат на активностите кои Владата преку ресорните министерства, како и другите државни институции и органи треба да ги преземат со цел отстранување на причините од утврдените неправилности, утврдените состојби или потенцијалните ризици, како и активностите кои треба да придонесат за надминување на утврдените слабости и обезбедат подобрување на безбедноста на информациските системи на субјектите кои имаат критична инфраструктура, особено во делот на достапноста, интегритетот и доверливоста на информациите кои ги обработуваат.

Прес контакт:
Албиона Мустафа Мухаџири +389 72228 203 albiona.mustafa@dzr.gov.mk
Мијалче Дургутов +389 70 358 486 mijalce.durgutov@dzr.gov.mk
Мартин Дувњак +389 75 268 517 martin.duvnjak@dzr.gov.mk