Почитувани,

Во контекст на последните случувања со ИКТ системот на ФЗОРСМ и неговата нефункционалност повеќе од 10 дена, сведоци сме на уште еден пример колку современиот начин на работење, наспроти сите предности и бенефиции е зависен од достапноста на дигиталните системи и колку сериозно ранливоста на овие системи може да влијае на нормалниот тек на функционирање.

За жал вакви настани во светот секојдневно се случуваат и од нив не е поштеден никој, ниту поединците, ниту пак организациите, од најмали до најголеми, доколку навреме не се преземаат соодветни заштитни мерки за нивно избегнување и намалување на потенцијалната штета доколку сепак се случат.

Навременото преземање на заштитни мерки и нивната правилна употреба се императив во борбата против компјутерскиот криминал и сајбер нападите, па во таа насока сакаме да Ви дадеме неколку препораки, со кои сметаме дека ќе допринесеме за Ваша поголема безбедност.

- **Внимателно ракување со е-маил пораки од непознати извори или со сомнителна содржина.** Не отварајте пораки од непознат испраќач, а доколку добиете порака и од познат контакт но со сомнителна содржина, не ги преземајте евентуалните прикачени фајлови. Конкретно, Ransomware нападите (од кои според информациите во медиумите е предизвикан инцидентот во системот на ФЗО) најчесто се вршат преку е-маил пораки.
- **Избегнувајте отворање на непознати веб страници,** како и веб страници со сомнителна содржина. Со отворање на вакви страници се ризикува упад на малициозен софтвер во Вашиот систем, кој потоа може да се прошири и по останатите работни станици во Вашата организација и да предизвика штета и евентуална загуба на податоци.
- **Антивирусен софтвер** – во денешно време антивирусната заштита представува задолжителен елемент во низата софтверски алатки кои треба да ги поседувате. Поради тоа препорачливо е сите работни станици кои ги користите(а доколку поседувате и сервер, истото важи и за него), независно дали во домот или на работното место да се соодветно заштиттени со антивирусен софтвер, кој е редовно ажуриран со последните надградби и дефиниции за справување со најновите компјутерски вируси.
- **Избегнувајте користење на сервер како работна станица** – со користењето на серверот на кој е инсталиран софтверот и каде се чуваат податоците како работна станица, ризикот од директнен напад на него е зголемен, поради директната изложеност на интернет страни и е-маил пораки до кои корисникот може да пристапи при употребата на работната станица. Поради тоа доколку е можно користете за сервер посебна хардверска единица.

- **Бекап на податоците** – Бекапот на податоците е критична активност која треба да ја применува секој корисник, независно дали е поединец или организација. Бекапот Ви дава можност да го реставрирате системот и Вашите податоци во случај истите да се делумно или целосно зафатени и оштетени од нападот.
  Независно дали ја користите нашата услуга за автоматизиран бекап, некоја друга услуга за бекап или пак сами го организирате бекап процесот, битно е при спроведувањето на бекапот тој да се врши барем еднаш дневно на работните податоци и копија од него да се чува и на издвоена локација. (Издвоена локација значи бекапот да не се наоѓа во рамки на системот чии податоци се зачувуваат, односно бекапот да биде ископиран на мемориски стик, преносен диск, FTP сервер или cloud локација како што нуди Google, Microsoft или DropBox). Со тоа драстично се намалува ризикот од загуба на податоци, бидејќи ќе поседувате валидна копија од Вашите податоци со минимален период на загуба од последниот бекап до моментот кога настанал инцидентот, а воедно ќе биде изводлива и операција на реставрација на податоците.

Со почит,

Кодекс Компјутери