ПОДИЗАЊЕ БЕЗБЕДНОСНЕ СВЕСТИ И КУЛТУРЕ У РАДУ СА ТАЈНИМ ПОДАЦИМА - СОЦИЈАЛНИ ИНЖЕЊЕРИНГ -

Социјални инжењеринг представља скуп техника манипулације људима ради добијања поверљивих информација или неовлашћеног приступа системима. У раду са тајним подацима људски фактор је најчешће најслабија карика. Због тога је развијање безбедносне свести и културе од суштинског значаја за заштиту националне безбедности. Запамтите: техничке баријере могу се заобићи; свест и дисциплина запослених представљају прву и последњу линију одбране.

ОСНОВНИ ОБЛИЦИ СОЦИЈАЛНОГ ИНЖЕЊЕРИНГА - Поред класичног фишинга (лажни мејлови), постоје и други облици напада на које је потребно обратити пажњу:

• **ВИШИНГ (Vishing)** – телефонски позиви са лажним идентитетом. Нападачи се представљају као колеге, техничка подршка или руководиоци и траже лозинке или податке.

• **СМИШИНГ (Smishing)** – SMS поруке или поруке преко апликација (Viber, WhatsApp) са линковима који воде ка злонамерним сајтовима.

• **ПРЕТЕКСТИНГ (Pretexting)** – лажно представљање и креирање измишљеног сценарија (нпр. „хитна контрола“) ради добијања поверљивих података.

• **БЕИТИНГ (Baiting)** – остављање „мамца“ у простору (USB меморија, CD, документ) који изазива радозналост и наводи запосленог да га прикључи или отвори.

• **ТЕЈЛГЕЈТИНГ / ПИГИБЕКИНГ (Tailgating)** – физички улазак у заштићени објекат праћењем овлашћеног запосленог, без сопствене идентификације.

• **ЗЛОУПОТРЕБА АУТОРИТЕТА** – позивање на „више инстанце“ или на хитност ради вршења притиска да се заобиђу процедуре.

НАПРЕДНЕ ТЕХНИКЕ И РИЗИЦИ

• **Социјалне мреже** – прикупљање информација о запосленима ради креирања персонализованих напада.
• **Емоционална манипулација** – изазивање осећаја хитности, страха или ентузијазма како би се искључило критичко размишљање.
• **Инсајдери** – запослени или сарадници који намерно или ненамерно откривају податке.
• **Физички приступ** – остављање лажних докумената или уређаја у просторијама институције.

ПОДИЗАЊЕ БЕЗБЕДНОСНЕ СВЕСТИ И КУЛТУРЕ У РАДУ СА ТАЈНИМ ПОДАЦИМА - СОЦИЈАЛНИ ИНЖЕЊЕРИНГ -

ПРИНЦИПИ ЗАШТИТЕ

• **НУЛТО ПОВЕРЕЊЕ (Zero Trust)** – сваки захтев за приступ мора бити верификован, без обзира на извор.

• **ВИШЕСЛОЈНА ОДБРАНА** – комбинација техничких, организационих и људских мера заштите.

• **РЕДОВНЕ ОБУКЕ** – практичне вежбе и симулације препознавања напада.

• **КУЛТУРА ПРИЈАВЉИВАЊА** – охрабривање запослених да одмах пријаве сумњиве активности, без страха од санкција.

• **МИНИМИЗАЦИЈА ПОДАТАКА** – приступ само оним информацијама које су неопходне за обављање задатка.

ПРЕПОРУКЕ ЗА ЗАПОСЛЕНЕ - Увек проверите идентитет лица које тражи приступ или информације, чак и ако се представља као познаник или руководилац. Не делите поверљиве податке (о поступцима јавних набавки, конкурсима, тајне и личне подакте, као и пословне и професионалне тајне) путем телефона, е-поште или друштвених мрежа без формалне верификације.

Не користите непознате USB уређаје, линкове или документе из непроверених извора.

Не допуштајте улазак у заштићене просторије особама без важеће идентификације.

Пријавите сваку сумњиву активност надлежном руковаоцу тајних или личних података.

Редовно освежавајте знање кроз обуке и тестове које организује орган јавне власти.

ЗАКЉУЧАК - Социјални инжењеринг није технички напад – он циља људе. Због тога је свест запослених кључна одбрана. Култура безбедности у институцијама мора се градити систематски, кроз едукацију, дисциплину и сталну проверу.

ПОРУКА:

„Човек или људски фактор је најслабија карика сваког система – али и најјача одбрана ако постоји свест и култура безбедности.“