Забеспячэнне абароны інфармацыі РУП «Белтэлекам»

У мэтах арганізацыі процідзеяння пагрозам інфармацыйнай бяспекі РУП «Белтэлекам» аказваюцца насельніцтву наступныя паслугі: абарона ад DDoS нападаў, фільтраванне сеткавага трафіку, прадастаўленне ліцэнзій на выкарыстанне антывіруснай аховы, павышэнне дасведчанасці ў сферы інфармацыйнай бяспекі, а таксама бацькоўскі кантроль.

Для папулярызацыі інфармацыйнай бяспекі створаны Інтэрнэт-партал: security.beltelecom.by, прысвечаны пытанням абароны інфармацыі.

У ходзе сваёй дзейнасці ў 2020 годзе спецыялісты прадпрыемства РУП «Белтэлекам» сутыкнуліся з наступнымі відамі пагроз:

1. Павялічылася інтэнсіўнасць размеркаваных нападаў, накіраваных на адмову ў абслугоўванні інфармацыйных сістэм і сетак.
2. Узрасла колькасць выпадкаў атрымання работнікамі прадпрыемства электронных паштовых паведамленняў, у якіх змяшчаецца шкоднаснае ўкладанне або спасылка на небяспечны («заражаны») інфармацыйны рэсурс (фішынг). Пры гэтым актыўна стала выкарыстоўвацца тэма пандэміі Covid-19.
3. Антывірусным праграмным забеспячэннем на сеткавым і канцавым абсталяванні РУП «Белтэлекам» фіксуюцца выпадкі наяўнасці шкоднаснага праграмнага забеспячэння (далей - ШПЗ). Вывучэнне выяўленага ШПЗ паказала яго арыентаванасць на выкраданне банкаўскай інфармацыі або шыфраванне даных. Пры гэтым павялічылася і хуткасць распаўсюджвання ШПЗ. Так у верасні 2020 года было апублікавана даследаванне ўразлівасці Zerologon (CVE-2020-1472), а ўжо ў кастрычніку 2020 года спецыялістамі РУП « Белтэлекам » зафіксаваны падобныя напады на інфармацыйныя сістэмы прадпрыемства.
4. Павялічыліся атакі, накіраваныя на канцавое сеткавае абсталяванне абанентаў. Выкарыстоўваючы перабор пароля (брутфорс) мадэмнага абсталявання, зламыснікі замацоўваюцца ў лакальнай сетцы абанента.
5. На канцавых прыладах абанентаў (камп’ютары, ноўтбукі, мабільныя прылады і інш.) працягваюць прысутнічаць розныя ўразлівасці і ШПЗ. Азначанае звязана з выкарыстаннем састарэлага або неліцэнзійнага праграмнага забеспячэння, ігнараванне легальнага набыцця і выкарыстання сродкаў аховы інфармацыі.

На думку спецыялістаў прадпрыемства, адным з фактараў паспяховасці праведзеных нападаў зламыснікамі з'яўляецца нізкі ўзровень пісьменнасці і дасведчанасці абанентаў у сферы інфармацыйнай бяспекі.

Пры вывучэнні сусветных тэндэнцый у сферы інфармацыйнай бяспекі з адкрытых крыніцаў (shodan.io, greynoise.io, censys.io і інш.) атрымана інфармацыя, якая сведчыць, што ў нацыянальным сегменце глабальнай сеткі Інтэрнэт значна павялічылася колькасць спроб «заражэння» IoT-прылад.