AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

BULETINI I LAJMEVE TË SIGURISË KIBERNETIKE

Maj 2020

PËRMBAJTJA:

Të paktën 460 milionë rekorde të dhënash u ekspozuan në incidentet breach gjatë muajit Maj.

Ndërkohë që muaji Prill u raportua si muaji me numrin më të ulët të rekordeve të ekspozuara si rezultat i sulmeve kibernetike (216 milionë) përgjatë 2020, muaji Maj arriti një shifër prej 8.8 miliardë rekorde të dhënash në total. Kompania IT Governance numëroi 105 incidente, nga ku më të rrezikshmet shënuan një numër prej 460 milionë rekordesh të ekspozuara.

https://www.itgovernance.co.uk/blog/list-of-data-breaches-cyber-attacks-may-2020

U zhvillua trajnimi CyberSec1.0 Theory2Practice

Për herë të parë në Shqipëri u zhvillua "CyberSec 1.0" Theory2Practice, për të trajnuar studentët më të mirë në degët e Teknologjisë së Informacionit, si dhe ekspertët e fushës së Sigurisë Kibernetike, e gjithë kjo në mbështetje të Autoritetit Kombëtar për CESK.

Një përpjekje sulmi nga hakerat regjistrohet çdo 39 sekonda

Një studim i Universitetit të Maryland tregon se në cdo 39 sekonda regjistrohet një sulm kibernetik. Këto përpjekje përfundojnë duke prekur 33% të rasteve të sulmuara çdo vit. Në të shumtën e rasteve, këto shifra vijnë pikërisht për shkak të përdorimit të fjalëkalimeve të dobëta dhe usernameve të pasigurta.

https://techrrival.com/top-cyber-security-facts/.

Google nxjerr programin për të luftuar mashtrimet e Coronavirus

Google nxori një program të ri për të luftuar mashtrimet që lidhen me pandeminë COVID-19, kjo pasi sulmet në internet dhe mashtrimet e phishing kanë spikatur gjatë krizës.

Programi i ri "Scam Spotter", i krijuar në bashkëpunim me Cybercrime Support Network, rekomandon një proces me tre hapa që individët duhet të marrin në konsideratë para se të dorëzojnë një informacion personal përmes një telefonate ose email.

https://cyware.com/news/capturing-the-cyber-threats-on- home-base-amidst-covid-19-99299e76

5 mënyra për të parandaluar sulmet në Internet

- Bëni kopje dhe back up të të dhënave dhe informacioneve të rëndësishme
- Instaloni, përdorni dhe përditësoni rregullisht antiviruset dhe antispyware në çdo kompjuter të përdorur në shtepinë apo biznesin tuaj.
- Përdorni firewall për lidhjen në internet.
- Shkarkoni dhe instaloni përditësimet e sistemeve operative dhe aplikacioneve sapo ato të jenë të disponueshme.
- Ndryshoni vazhdimisht fjalëkalimet.

https://capcoverage.com/index.php/10-ways-to-prevent-cyber-attacks

Lulëzojnë sulmet kibernetike në e-commerce gjatë pandemisë COVID-19

Gjatë pandemisë COVID-19, sofistikimi i sulmeve në internet është shumëfishuar dhe e-commerce është një nga segmentet më të goditura prej tyre, kjo për shkak se ruhen informacione të payment card-eve të klientëve. Për pasojë, hakerët kanë përfituar 1.6 milion dollarë nga shitja e më shumë se 239,000 rekordeve të payment card-eve në Dark Web.

https://cyware.com/news/cyber-threats-loom-on-the-e-commerce-sector-during-covid-19-epidemic-7725e7a4

Pagesa për ransomware nënkupton dyfishim kostosh

Sipas FBI, asnjë person ose organizatë nuk duhet të paguajë kurrë për rikthimin e të dhënave nga sulmet ransomware. Të parandalosh një sulm ransomware kushton mesatarisht më shumë se 730,000 $ në 1 vit,por kjo shifër rritet në 1.4 milion dollarë kur organizatat vendosin të paguajnë vlerën që sulmuesit kërkojnë.

https://cyware.com/news/why-pay-ransom-when-you-can-avoid-it-9f7b9384

Kujdesi për sigurinë tuaj në rrjetet sociale

- Informacionet që ju shpërndani janë shumë të rëndësishme për dikë që do t'ju bëj keq. Sulmuesit përdorin të dhënat që ju postoni në rrjetet tuaja sociale për të vjedhur identitetin tuaj.
- Mundohuni të evitoni publikimin e informacioneve si ditëlindje apo vendodhjen tuaj, të cilat shpeshherë janë publike në rrjete sociale.
- Kur postoni fotografi në evente apo vende të ndryshme, ju praktikisht po u tregoni sulmuesve që nuk jeni në shtëpi, kështu është më e lehtë për ta të planifikojnë vjedhje apo sulme. Gjithmonë, publikoni fotografi të pushimeve tuaja atëherë kur jeni të sigurt në shtëpi.
- Sulmues të ndryshëm përdorin median sociale që të krijojnë lidhje me fëmijë, prandaj prindërit duhet t'i monitorojnë dhe të jenë sa më të kujdesshem për rrjetet sociale të fëmijëve të tyre.

Sulmet kibernetike përhapen me shpejtësi në sektorin e arsimit

Sektori i arsimit është një objektiv tërheqës për kërcënuesit. Shumë institucione shtetërore e kanë të vështirë të investojnë në sigurinë e IT, duke i bërë ata të prirur për tu sulmuar, sidomos nga sulmet ransomware.

https://capcoverage.com/index.php/10-ways-to-prevent-cyber-attacks/

Kuadri Ligjor i sigurisë së informacionit në Shqipëri

- **Hacking-** Përbën krim sipas Kushtetutës së Republikës së Shqipërisë, ku përdorimi i paautorizuar i një Sistemi Informacioni ose pjesëve të saj, dënohet me gjobë e deri në tre vite burg
- **Denial Of Service-** Krijimi i pengesave serioze dhe të paautorizuara për të cenuar funksionimin e një sistemi kompjuterik, nëpërmjet futjes, dëmtimit, shtrembërimit, ndryshimit, fshirjes apo suprimimit të të dhënave, dënohet me burgim nga tre deri në shtatë vjet.
- **Phishing-**Futja, ndryshimi, fshirja ose heqja e të dhënave kompjuterike apo ndërhyrja në funksionimin e një sistemi kompjuterik, me qëllim për t'i siguruar vetes apo të tretëve, me mashtrim, një përfitim ekonomik të padrejtë apo për t'i shkaktuar një të treti pakësimin e pasurisë, dënohen me burgim nga gjashtë muaj deri në gjashtë vjet.
- **Infektmi i sisteme të informacionit me malware-** Dëmtimi, shtrembërimi, ndryshimi, fshirja apo suprimimi i paautorizuar i të dhënave kompjuterike dënohen me burgim nga gjashtë muaj deri në tre vjet

http://www.pp.gov.al/web/kodi_penal_2017_1200.pdf