UBT - CERT
unit / division

DRAFT PROPOZIM: STRATEGJIA SHTETËRORE PËR SIGURI KIBERNETIKE DHE PLANI I VEPRIMIT TË NJË SHTETI

Veton Bejtullahu, Blent Kurtalani
UBT-CERT
08.06.2017

PËRMBAJTJA

HYRJE

- Si pjesë e një rritje të vazhdueshme të një bote të ndërlidhur mes veti në internet, shteti, infrastrukturat, bizneset dhe të gjithë njerëzit varen nga funksionimi i besueshëm i teknologjisë së informacionit dhe komunikimit.
- Liria dhe vlera e njerëzve në botën kibernetike duhet mbrojtur ashtu sikur në botën e jashtme. Institucionet qeveritare luajnë rol kryesor duke përcaktuar politika dhe udhëzime, për të siguruar hapësirën kibernetike.
- Sot, secili shtet i zhvilluar ka një strategji të sigurisë dhe plan të veprimit për 3 apo 4 vitet në vazhdim.

VIZIONI

- Aftësia për garantim të një sigurie nacionale dhe mbështetje në funksionimin e një shoqërie gjithëpërfshirëse, të hapur dhe të sigurtë.
- Hapja e laboratorit të forensikës
- Bashkëpunim me partnerët vendorë dhe ndërkombëtarë.
- Ekonomi dhe infrastrukturë dixhitale

ANALIZA

- Me numrin e përdoruesve në internet gjithmonë në rritje, dhe me teknologjitë e reja, numri i mundësive për sulm së bashku me kompleksitetin e sulmit, po rritet gjithashtu.
- Rreziku kryesor mbetet krimi kibernetik dhe rritja e tij reflektohet nga zhvillimi i shkathtësive të kriminelëve kibernetik dhe aftësia e tyre për të bërë sulme të organizuara.
- Infrastrukturat kritike që mund të sulmohen janë: sistemi energjetik, sistemi financiar, ujësjellësi, telekomunikacioni, siguria dhe rendi publik.

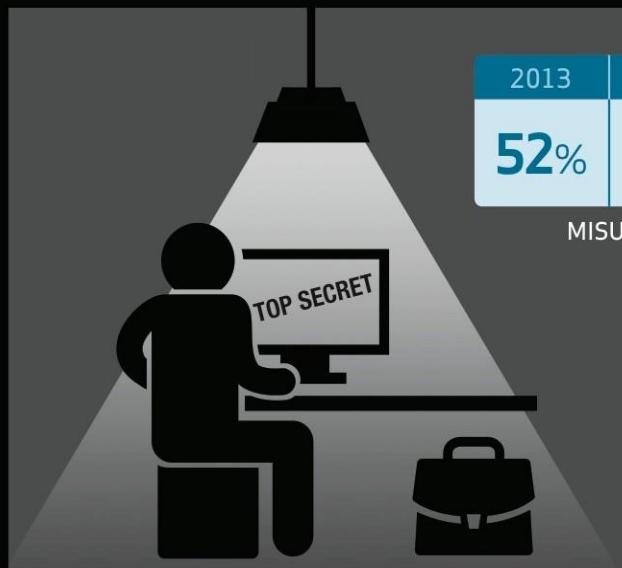
OBJEKTIVAT

- Ruajtje e të dhënave të publikut, kompanive dhe institucioneve qeveritare.
- Mbrojtje e infrastrukturave kritike të informacionit.
- Sigurim i sistemeve të IT në administratën publike.
- Qendër e reagimit kibernetik.
- Fushata vetëdijësuese të institucioneve dhe publikut për rreziqet dhe sulmet kibernetike.
- Stimulim i hulumtimeve dhe zhvillimeve në këtë fushë.

CYBER SECURITY THREAT PREVENTION

TOP FIVE CYBER THREATS TO GOVERNMENT AGENCIES

52%	49%	47%	42%	39%
MISUSE	PHISHING	MALWARE	SPAM	DATA LEAKAGE



	2013	2012
MISUSE	52%	40%
MALWARE	47%	59%
CYBER ESPIONAGE	15%	25%

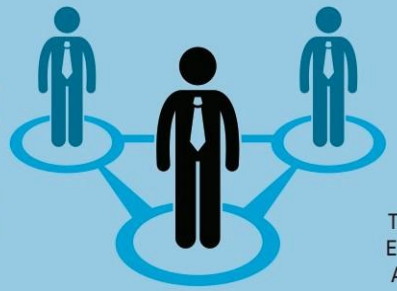
MISUSE HAS INCREASED SIGNIFICANTLY SINCE 2012

MALWARE AND CYBER ESPIONAGE HAVE DECREASED

LACK OF TRAINING IS AN OBSTACLE TO CYBER THREAT PREVENTION

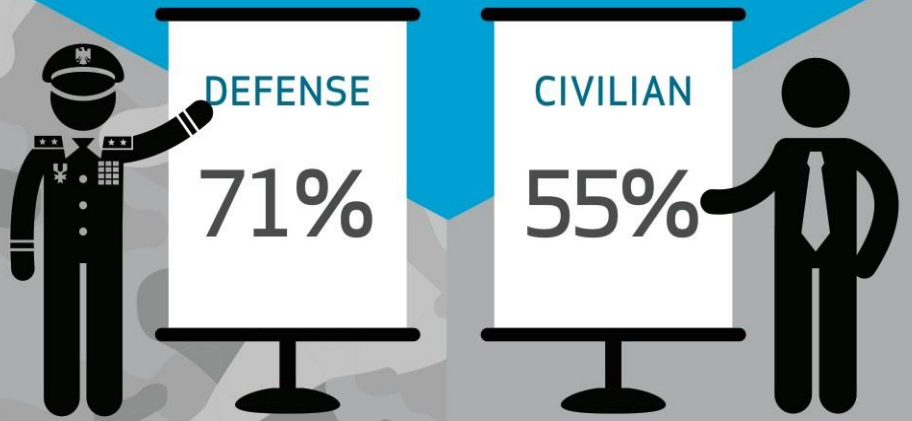
Almost 70% agree that end users are aware of agency security policies, yet lack of training is an issue

32% LACK OF TRAINING FOR SUPERVISORS IS AN OBSTACLE



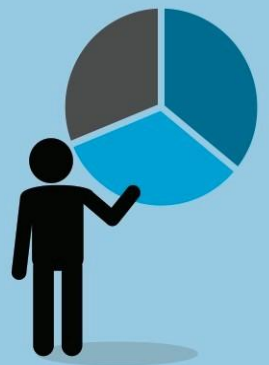
28% LACK OF SECURITY TRAINING FOR EMPLOYEES IS AN OBSTACLE

EMPLOYEE TRAINING IS A SIGNIFICANTLY HIGHER INVESTMENT PRIORITY FOR DEFENSE AGENCIES



EMPLOYEE TRAINING

IS A TOP INVESTMENT PRIORITY FOR PREVENTION OF CYBER THREATS



- **66%** IMPLEMENTATION OF TECHNICAL/SYSTEM SAFEGUARDS
- **61%** EMPLOYEE TRAINING
- **57%** POLICY/PROCEDURE IMPLEMENTATION OR CHANGES

IMPLEMENTIMI

- Adresimi i çështjeve thelbësore për menaxhimin e krizës kibernetike dhe propozimi i masave për efikasitet më të lartë.
- Analizim i raporteve mbi gjendjen e sigurisë të paraqitura nga grupi koordinues i sigurisë kibernetike.
- Lëshim i vlerësimeve periodike mbi gjendjen e sigurisë.
- Përcaktimi i planeve të veprimit për kriza kibernetike.
- Edukim shtesë, për të krijuar gjeneratën e ardhshme të profesionistëve në siguri kibernetike.

MONITORIMI

- Koodrinatori Nacional i Sigurisë Kibernetike monitoron indikatorët e Strategjisë.
- Ministritë dhe institucionet tjera monitorojnë aktivitetet që u janë ndarë atyre dhe dorëzojnë raportet periodike tek Koordinatori Nacional.
- OJQ duke qenë pjesë e tryezave të rrumbullakëta gjithashtu monitorojnë dhe paraqesin rekomandimet në lidhje me gjendjen e sigurisë.
- Koordinatori Nacional përpilon një raport në fund të çdo viti, sa i përket numrit të aktiviteteve, projekteve, personelit dhe strukturave.

VLERËSIMI

- Raporti vjetor i zbatimit të Strategjisë
- Anketa për nivelin e njohurisë nga publiku si rezultat i fushatave të vetëdijësimit për sigurinë kibernetike.

PLANI I VEPRIMIT

- Reflekton përpuethshmërinë me kornizat e përcaktuara me Strategjinë Shtetërore për Siguri Kibernetike.
- Rishikohet në çdo fundvit, që të sigurohet zbatueshmëria e Strategjisë.
- Përfshihen:
  - Aktivitetet
  - Afati kohor
  - Buxheti
  - Institucioni përgjegjës
  - Institucionet mbështetëse
  - Indikatorët e performancës