



Univerza v Mariboru

Fakulteta za varnostne vede

Varno poslovanje v kibernetskem prostoru

Igor Bernik, Univerza v Mariboru
Fakulteta za varnostne vede

9. posvet dolenjskih in belokranjskih informatikov, marec 2016





Odvisnost poslovnega sistema od IT

Je v sodobnem poslovanju popolna.

Problematika varnosti

- Splošna,
- omrežna in
- osebna.

Stanje

Stanje na področju kibernetске varnosti je z vidika ogroženosti **kritično**.

Imamo neizkoriščene možnosti:

- Nadgradnje varnostnih tehnologij
- Izboljšave procesov in postopkov varovanja
- Opismenjevanja uporabnikov in dvig zavedanja na področju preprečevanja delovanja kibernetских kriminalcev.



Prihajajoče tehnologije

- IOT – Internet of Things
- BYOD in nosljive naprave
- Kibernetski terorizem in problem migracij
- Big data

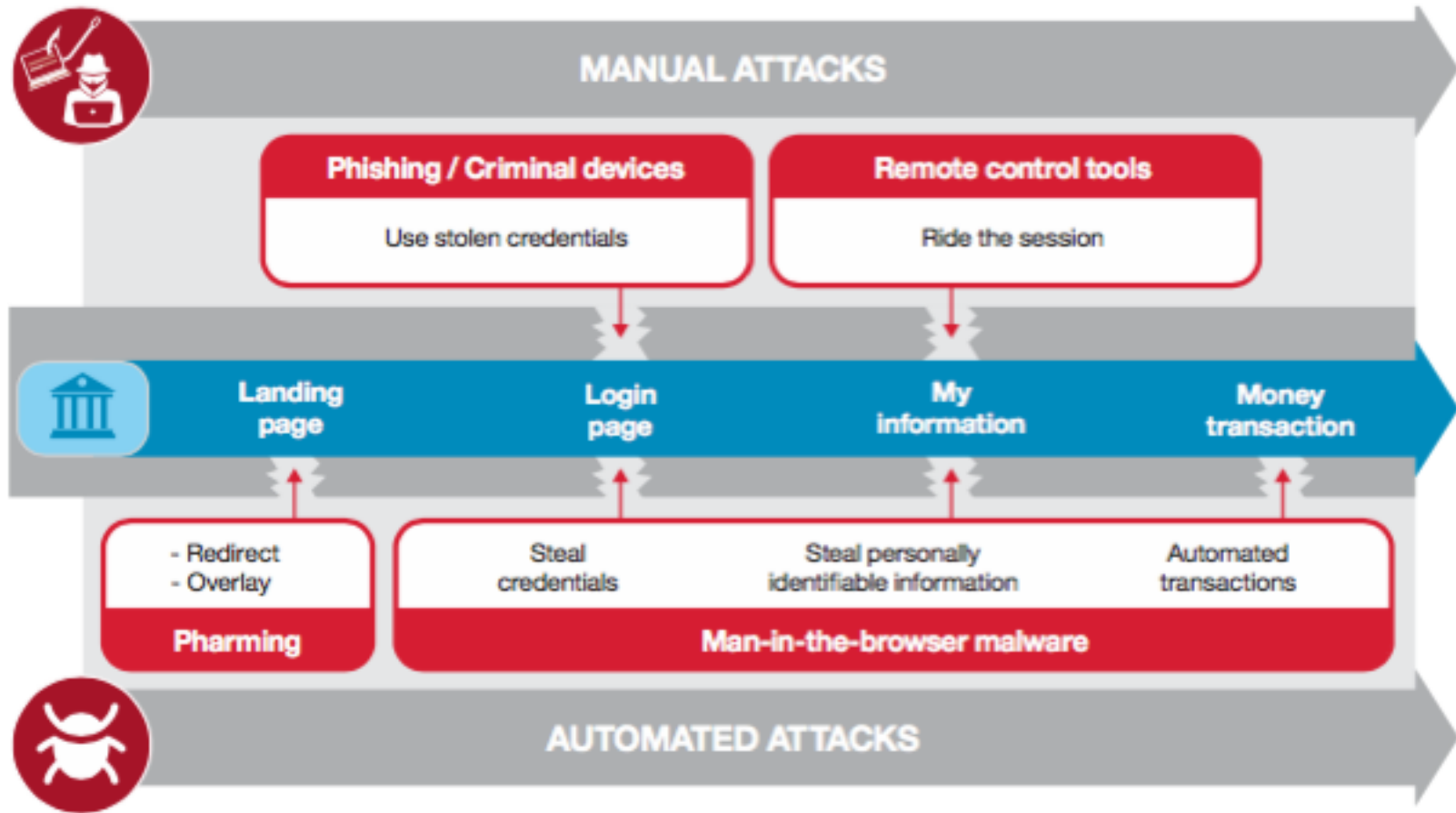


Zavarovanje premoženja

Vrednost organizacije z vidika kibernetске varnosti:

- Popis sredstev
 - Različni strežniki
 - Dostop do interneta
 - VPN konzentradorji
 - Vse STREŽNIŠKE domene.
- Podatki (kaj imamo, kje, tip)
- Vrednost (fizičnih sredstev in podatkov)
- Stroški regulative in pravnih omejitev
- Odgovornost in/ali lastništvo, kontrole

Napadi – povzročanje škode





Načrt odzivanja (action plan)

... na incidente

- Identifikacija tveganj nima smisla, če nimamo načrta odzivanja na incidente
- Načrt odzivanja je “živ” dokument, ki opredeljuje in nadgrajuje odzive na uresničitev možnih tveganj.
 - Upoštevati mora vse (nove) grožnje in ranljivosti sistema.



Načrt odziva

Načrt odziva na incidente črpa izhodišča iz registra tvegnaj in ciljev organizacije ter popisuje odzive na vsa opisana tveganja.

S tem pridobimo:

- Najprimernejše načine odzivanja, osnovane na analizi stroški/koristi
- Opis akcij za zmanjšanje tveganj
- Opis postopkov v primeru incidentov (krizni načrt)
- Dodeljene odgovornosti in časovni okvir za vsak odziv
- Zagotavljanje podrobnosti in ključno osebje in agencije, ki jih seznanimo v času ali po odpravi tveganj.



Prihodnost kibernetских napadov

- Usmerjeni napadi se bodo povečevali, splošni zmanjševali
- Kraja identitete v socialnih omrežjih
- Kombinirani postopki napadov
- Naraščanje napadov na mobilne naprave
- Omrežni promet je/bo nemogoče nadzirati
- Zadrževanje je nov način preventive
- Naraščanje napadov povezanih s posameznimi dogodki
- Socialni inženiring
- “Mobilna” škodljiva koda ogroža uporabnike in organizacije
- Ponovna uporaba poznane škodljive kode
- Napadi na storitve v oblaku



Sklep

Priložnosti zlorab so odprte, kriminalne združbe pa zavzeto izkoriščajo novosti in neukost uporabnikov.

Prihodnost kibernetске varnosti bo zahtevala simbiozo med ljudmi in tehnologijo.

“Novi svet” potrebuje nove rešitve!



Projekt

Varnostno opismenjevanje uporabnikov v kibernetickem prostoru – temelj varne prihodnosti (v nadaljevanju VarKib)

izbran na javnem razpisu za soofinanciranje in vzpostavitev e-storitev in mobilnih aplikacij na področju napredne uporabe ikt v izobraževanju 2014-2015 in je soofinanciran s starni Republike Slovenije Ministrstva za šolstvo in šport ter Evropske sheme »Naložba v prihodnost«.



Univerza v Mariboru

Fakulteta za varnostne vede



REPUBLIKA SLOVENIJA
MINISTRSTVO ZA IZOBRAŽEVANJE,
ZNANOST IN ŠPORT



Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj