Kibernetska (ne)varnost v Sloveniji

Matjaž Pušnik - PRIS, CISA, CRISC

KPMG

Agenda

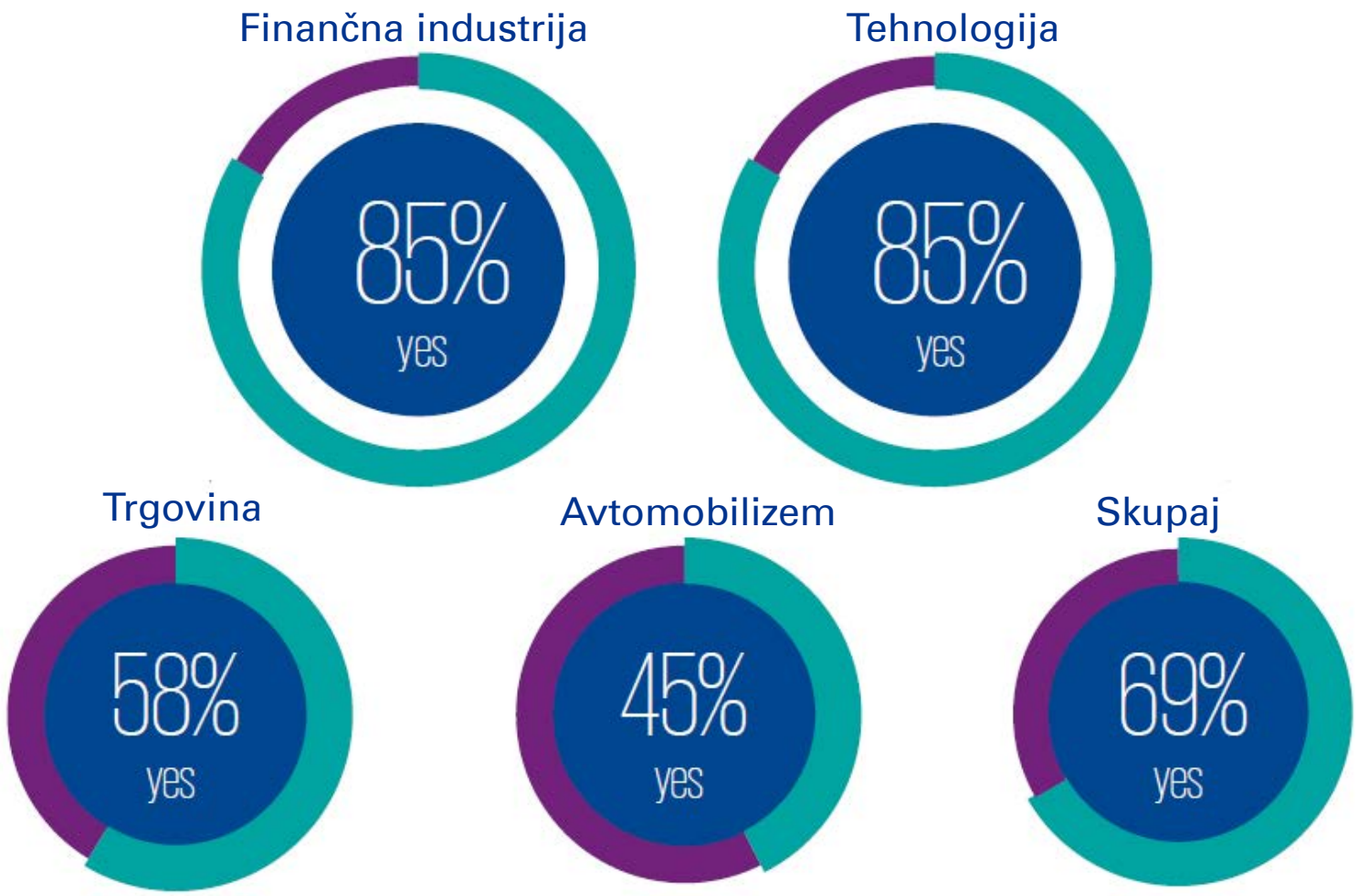
Poslovni vidik

Kibernetska varnost

Zakonodaja

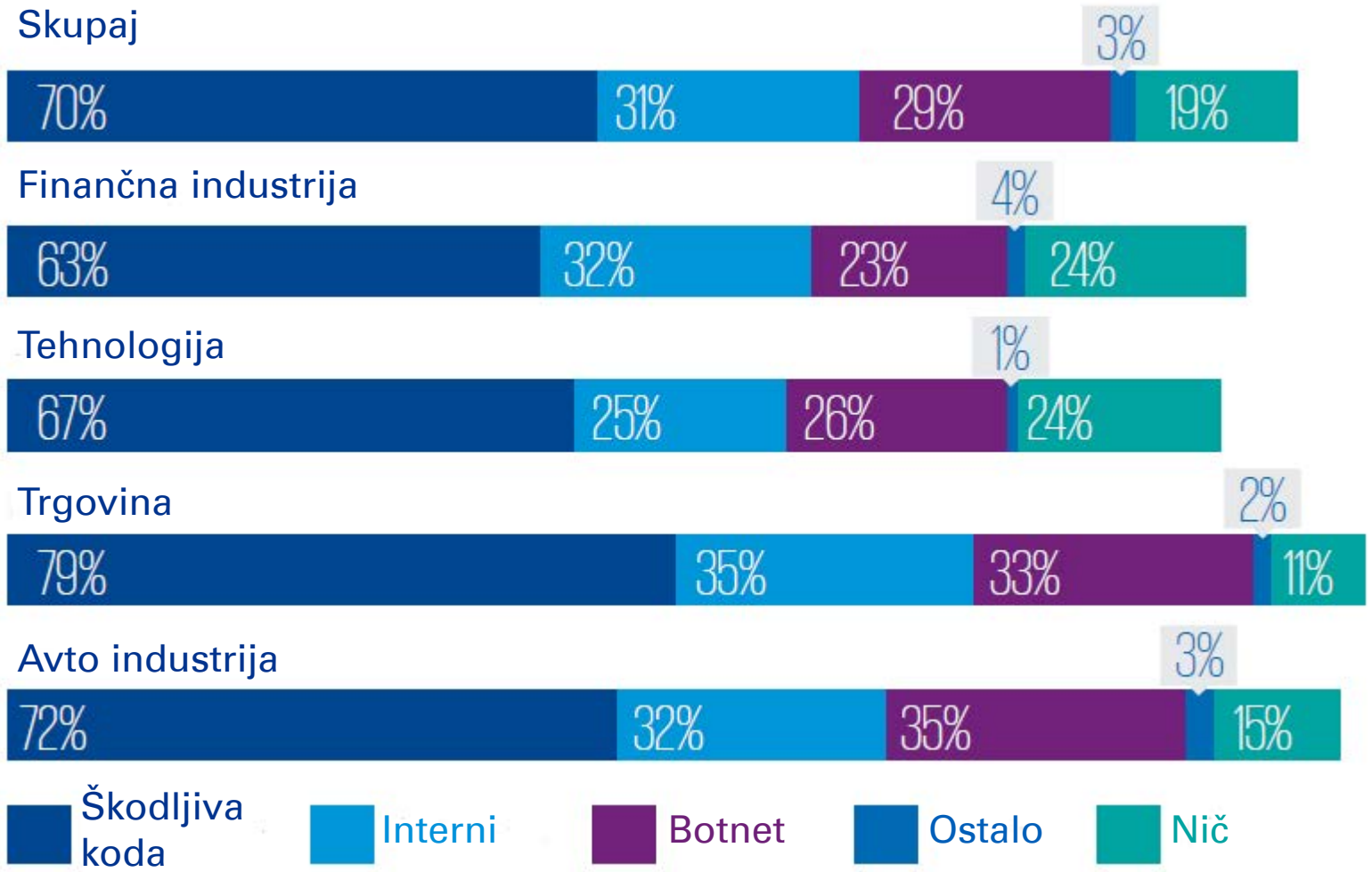
Zaključek

Ali imate vodjo, ki je zadolžen za varovanje informacij?



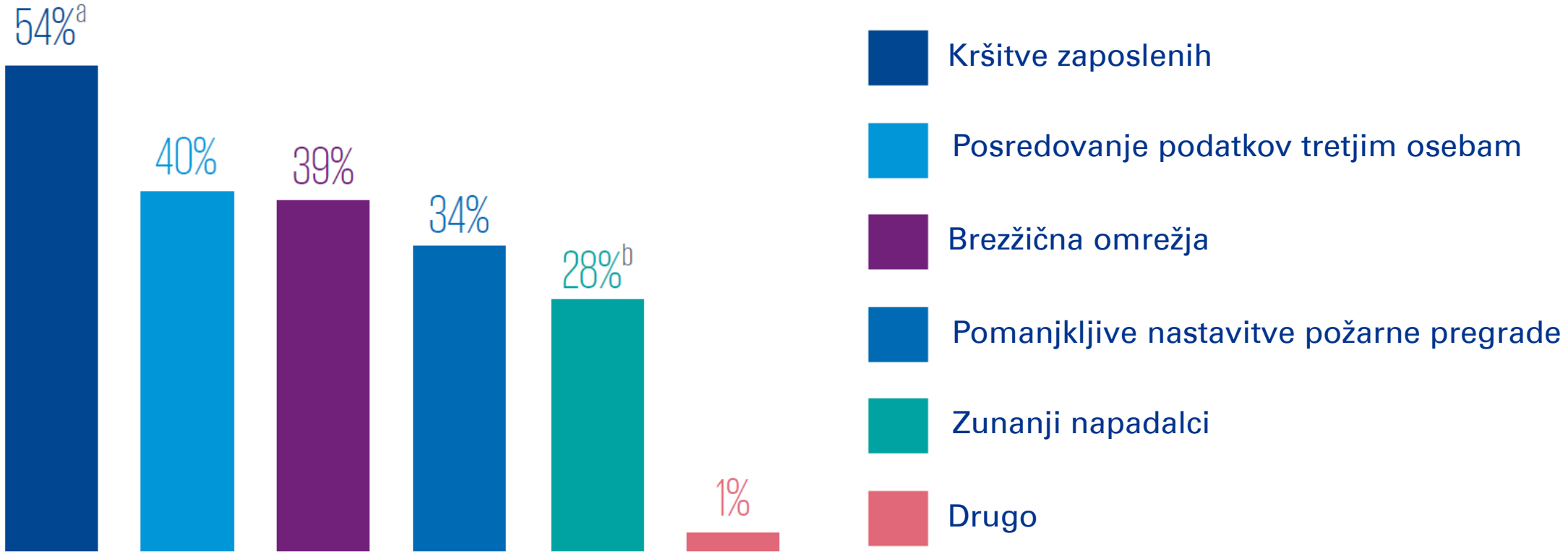
Consumer loss barometer
KPMG

Varnostni napadi v zadnjih 2 letih



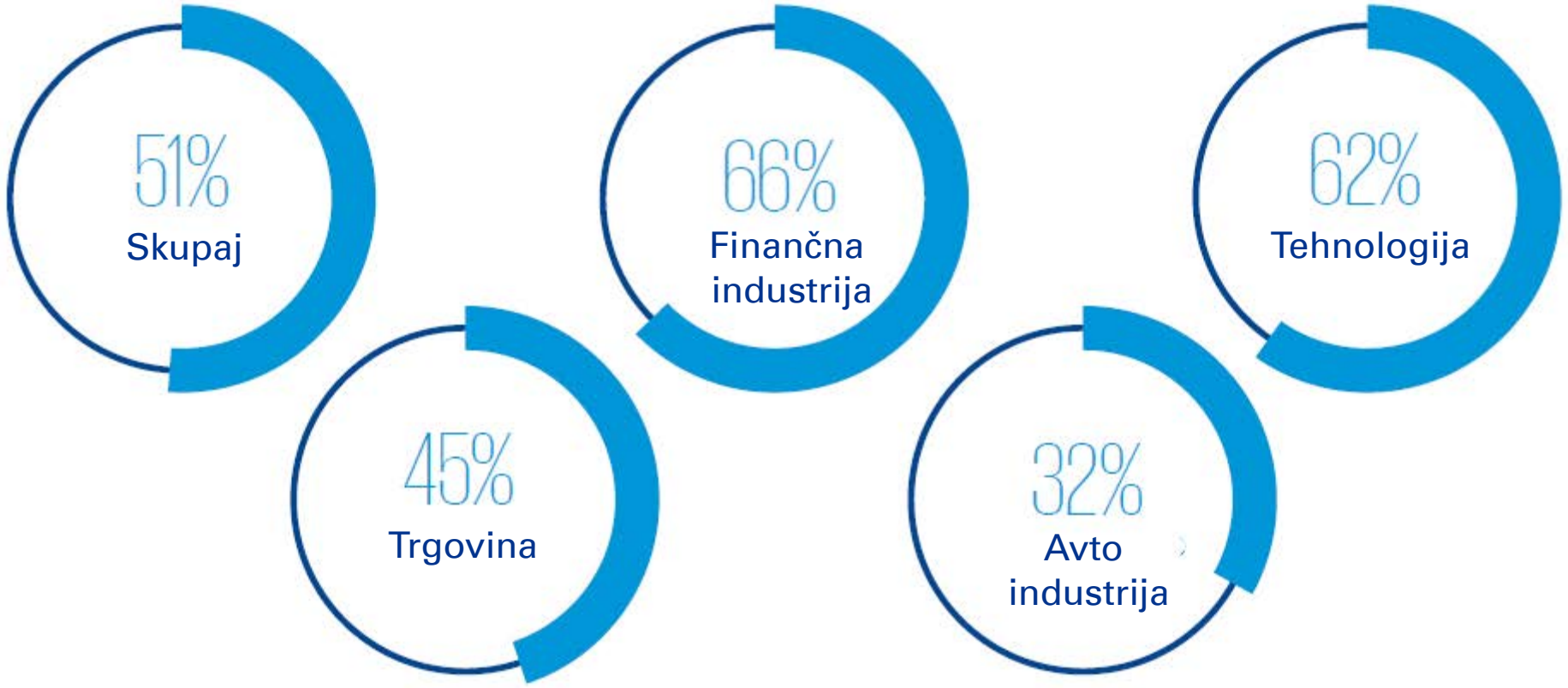
Consumer loss barometer KPMG

Zaposleni so najšibkejši člen kibernetske varnosti



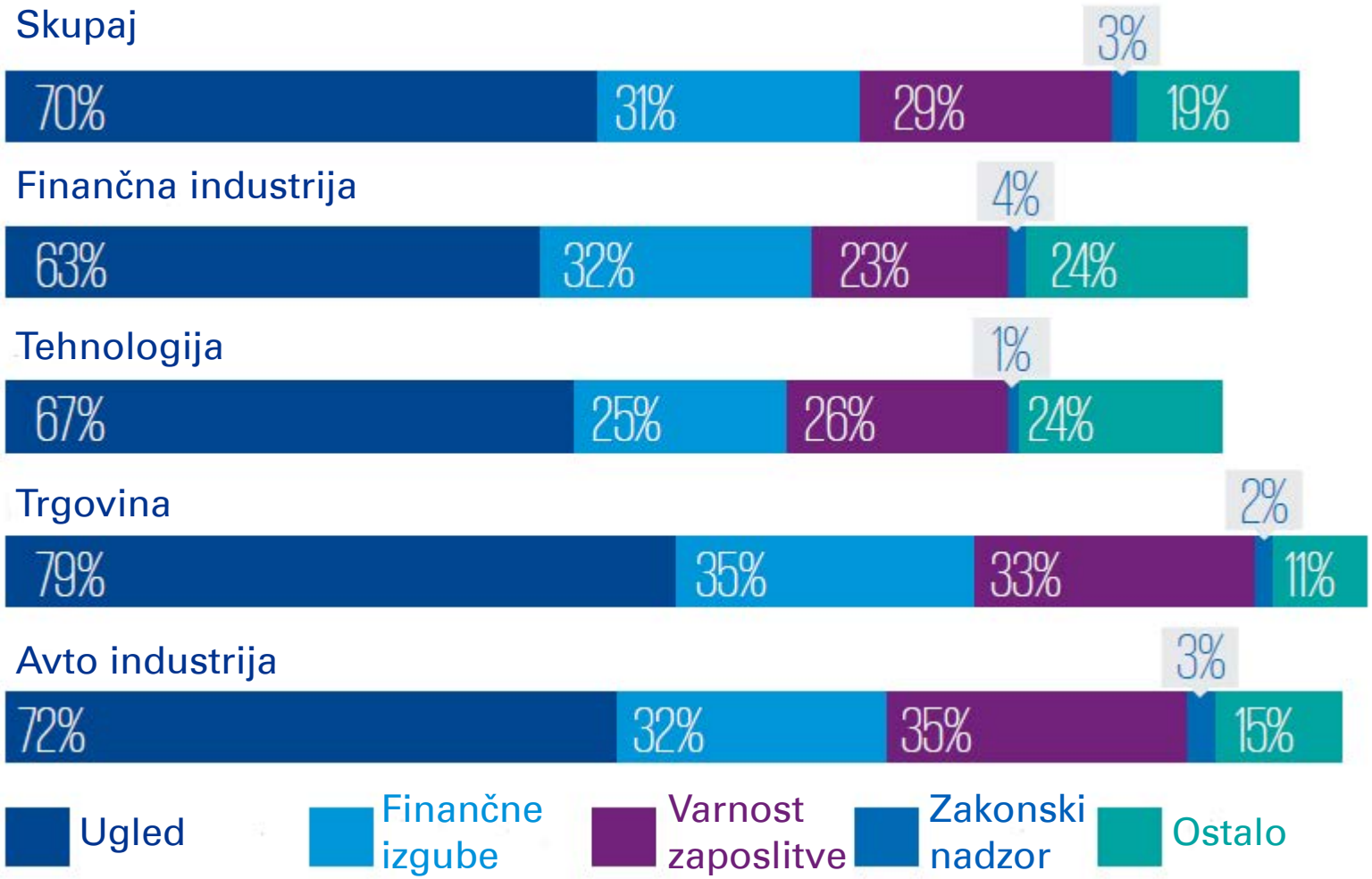
Consumer loss barometer
KPMG

Investicije za zagotavljanje kibernetske varnosti



Consumer loss barometer KPMG

Večja tveganja in stroški



Consumer loss barometer KPMG

Kibernetska varnost

Slovenija

Stanje

— Več podatkov, slabše obvladovanje in razumevanje podatkov

— Večje zahteve in pričakovanja zakonodajalcev ter trga (strank)

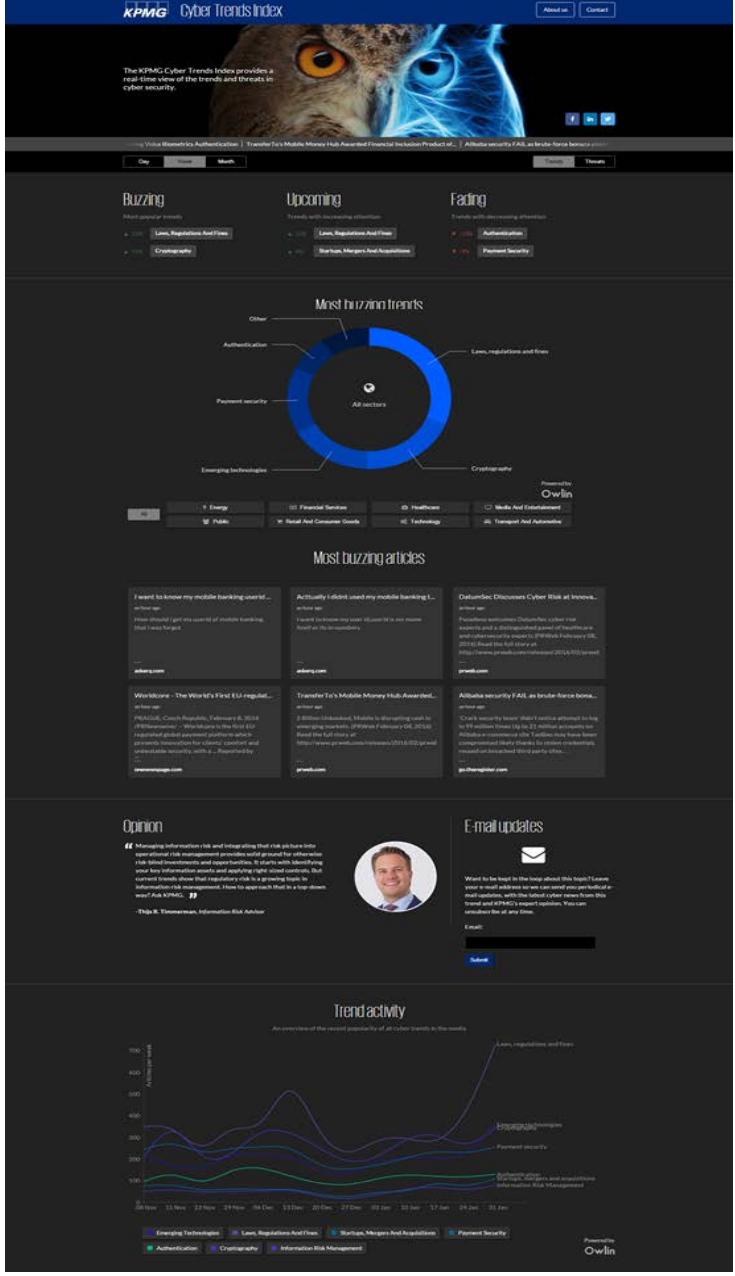
— Stroški kraje in kršitve podatkov strmo naraščajo

— Višji stroški zagotavljanja skladnosti

— Upravljanje v „silosih“

— Organizacijske spremembe

— Globalizacija



Ključna vprašanja

Katere so najnovejše grožnje in tveganja in kako vplivajo na organizacijo?

Ali je naš kibernetski varnostni program pripravljen na današnje in izzive prihodnosti?

Katere ključne kazalnike bomo spremljali na operativnem in vodstvenem nivoju za učinkovito upravljanje kibernetskih tveganj?

Varnostni profil

Zaposleni, Procesi in Tehnologija

Kibernetska varnost je več kot tehnološki problem!

Program kibernetske varnosti

— Zmanjšanje tveganja napada od zunaj in posledic uspešnega napada

— Boljše odločitve na področju kibernetske varnosti

— Jasno komuniciranje o kibernetski varnosti

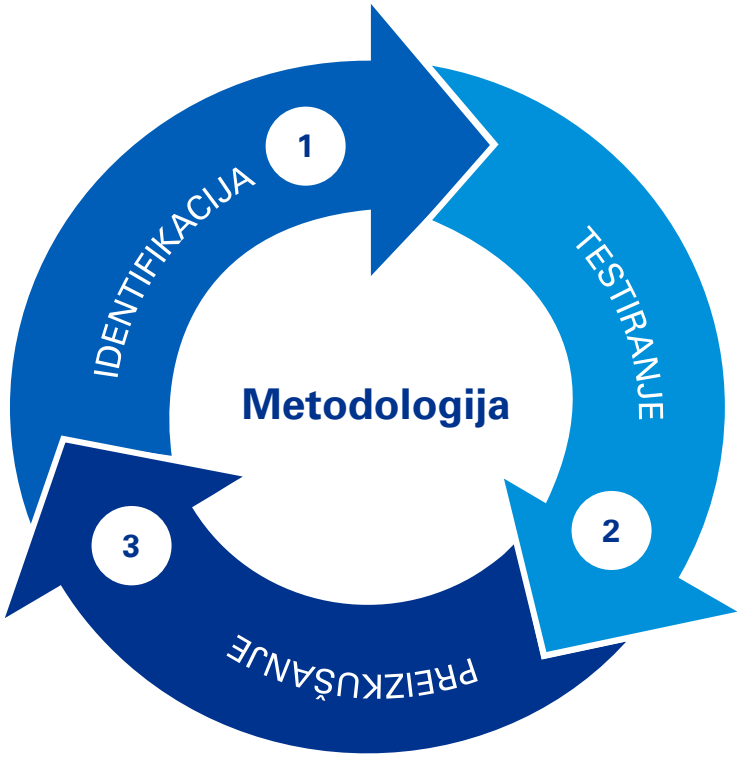
— Zaščita dobrega ugleda

— Izboljšanje znanja in kompetenc

— Primerjava stanja glede na industrijo

Metodologija

1. Identifikacija – sistemov in storitev
2. Testiranje – odkrivanje ranljivosti sistemov in storitev
3. Preizkušanje – izkoriščanje ranljivosti



Tehnike testiranja kibernetske varnosti

Zakonodaja in standardi

Evropska zakonodaja

Slovenska zakonodaja

Standardi

Dobre prakse

Zakonodaja - varovanje osebnih podatkov

25.5.2016 - Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov

Pomembno

Nova pravila o varstvu osebnih podatkov v EU

- Pravice posameznika
- Obveznosti upravljavcev in obdelovalcev podatkov
- Nadzorni organi
- Pravica do pravnega sredstva in sankcije
- Kodeksi ravnanja in potrjevanje (certifikacija)

Rok za prenos v nacionalno zakonodajo **25.5.2018**

Pomembno za varovanje osebnih podatkov

Večje kazni

Uredba vpeljuje kazni do 20 milijonov EUR ali 4% letnega prometa (lahko tudi več pri podjetjih, ki imajo promet večji od 500 milijonov letno).

Zelo velika in resna sprememba glede na trenutne nizke kazni.

Večje tveganje ugleda

Število pregledov povezanih z varstvom osebnih podatkov se bo zelo povečalo. Kršitve/kraje osebnih podatkov bodo hitreje javno razkrite.

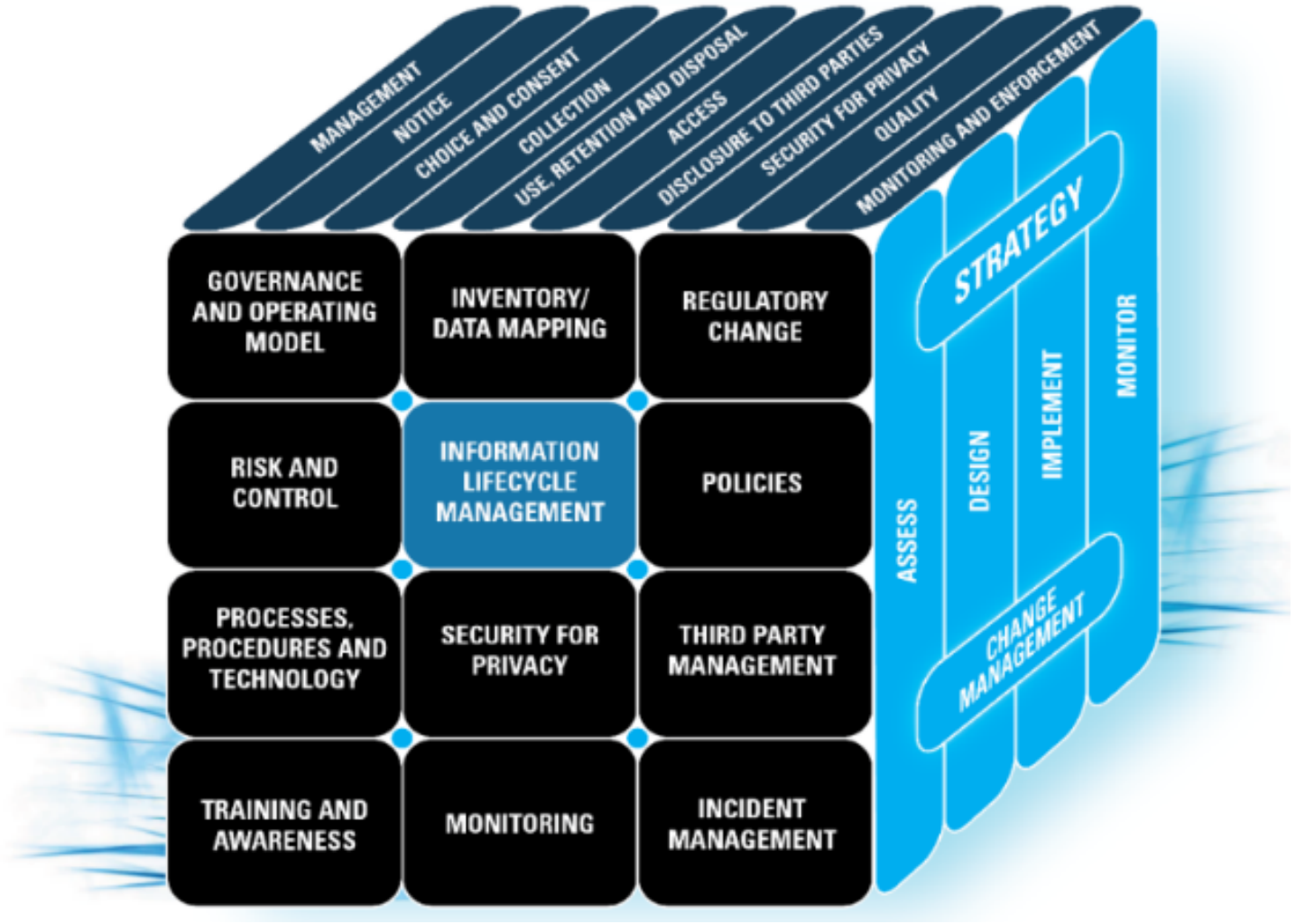
Tveganje ugleda bo prišlo še bolj v ospredje.

Večji svetovni doseg

Nova zakonodaja ima večji svetovni doseg in se je razširilo na ‘all organizations offering goods or services to EU citizens’ in ‘organizations that monitor (online) behaviour of EU citizens’.

Veliko več organizacij bo moralo izpolnjevati EU zahteve.

Orodja



Hitre zmage

1. Hitri pregled skladnosti z zakonodajo
2. Hitri pregled upravljanja varstva osebnih podatkov
3. Hitra ocena zrelosti varovanja osebnih podatkov
4. Pregled implementacije varovanja osebnih podatkov

Zaključek

Zmote kibernetske varnosti

1. **Dosegli bomo 100% varnost**
   100% varnost ni možna in ni realen cilj.

2. **Nakup najboljše tehnologije nam zagotavlja varnost**
   Učinkovita kibernetska varnost je manj odvisna od tehnologije kot si mislimo.

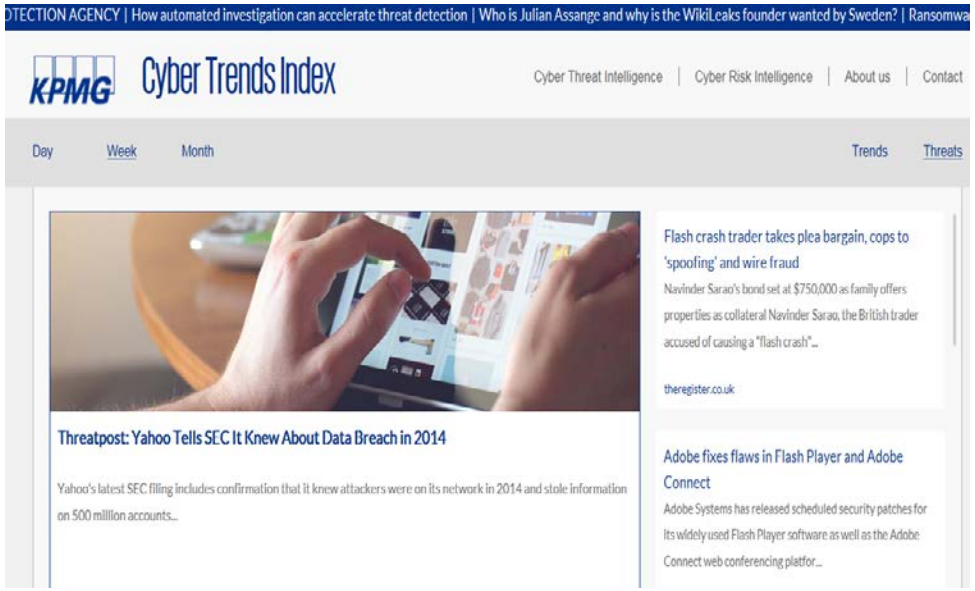
3. **Naše orožje mora biti boljše od napadalcev**
   Varnostna politika mora zasledovati cilje organizacije in ne ciljev napadalcev.

4. **Za zagotavljanje skladnosti kibernetske varnosti je dovolj učinkovit nadzor**
   Zmožnost učenja je enako pomembno kot nadzor.

5. **Zaposlitev najboljših strokovnjakov, bo ustavila kibernetske nevarnosti**
   Ključen je pristop, saj kibernetska varnost ni organizacija.

Razvoj

KPMG Cyber Trends Index



http://cyber.kpmg.com

— Pregled objave varnostnih dogodkov v realnem času

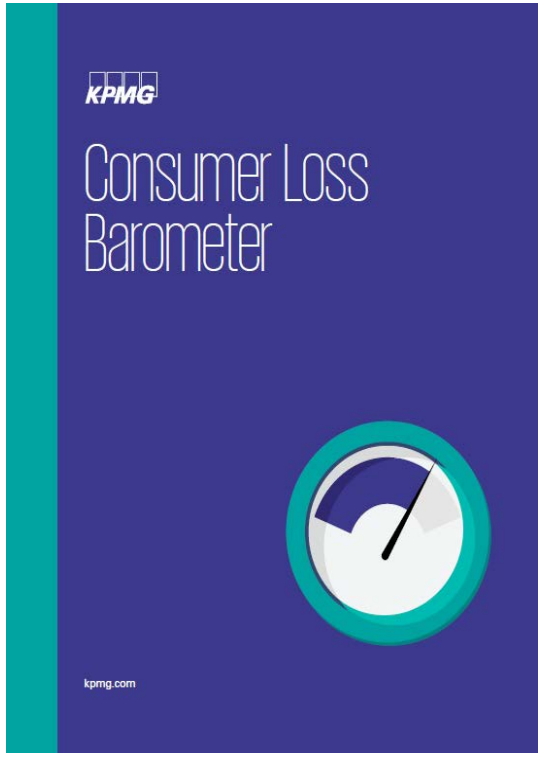
— Novice, trendi, nove ranljivosti in rešitve

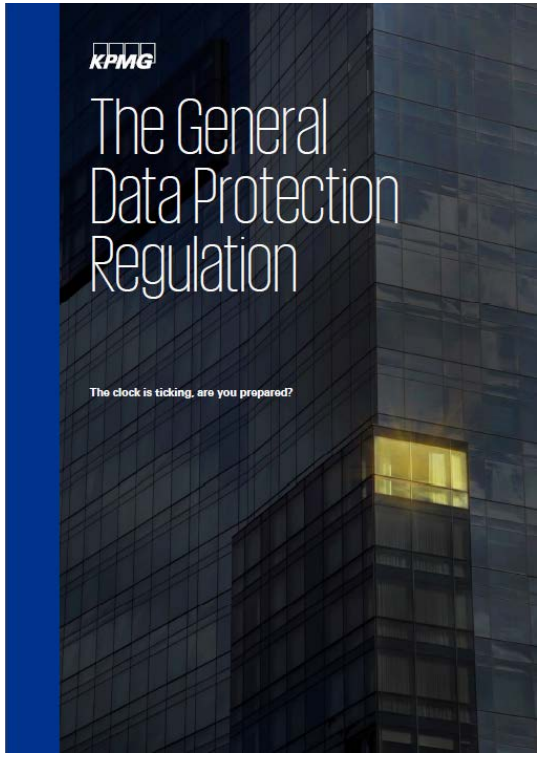
— Spremljanje kibernetskih napadov

Matjaž Pušnik
Manager, IT svetovanje in revizija
KPMG Slovenija

T: +386 1 236 43 35
E: matjaz.pusnik@kpmg.si

kpmg.com





Hvala

Matjaž Pušnik

KPMG

matjaz.pusnik@kpmg.si