



Kibernetska (ne)varnost v Sloveniji

Matjaž Pušnik - PRIS, CISA, CRISC

KPMG

CISCOSEC

Agenda

Poslovni vidik

Kibernetska varnost

Zakonodaja

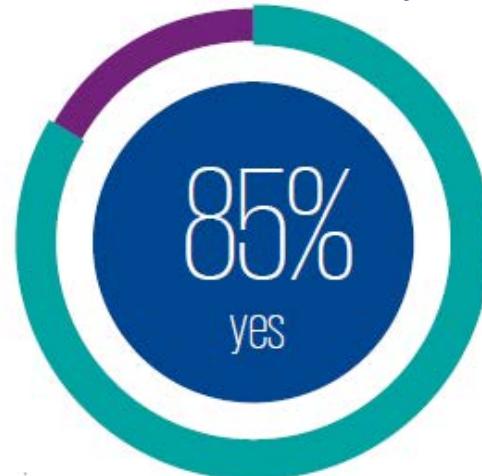
Zaključek



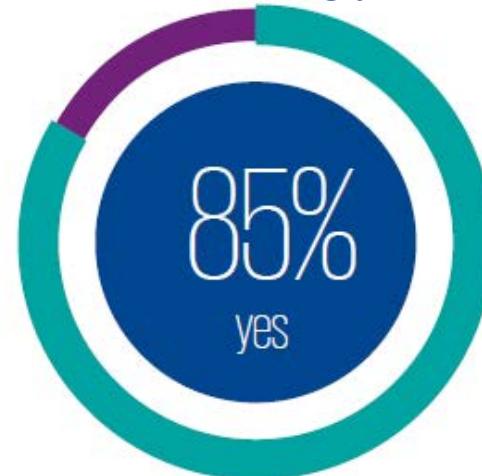
© 2016 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

Ali imate vodjo, ki je zadolžen za varovanje informacij?

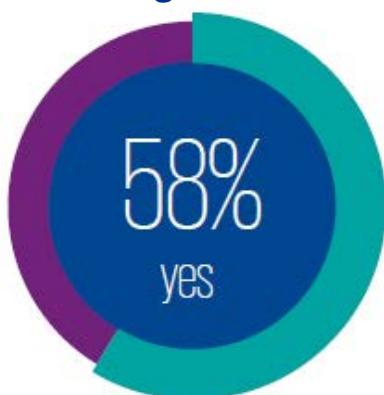
Finančna industrija



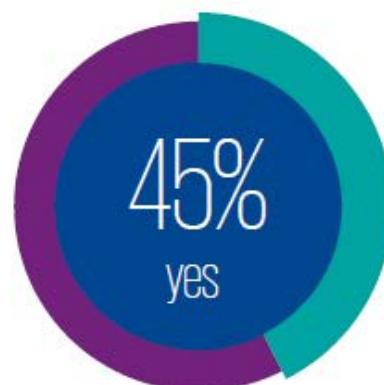
Tehnologija



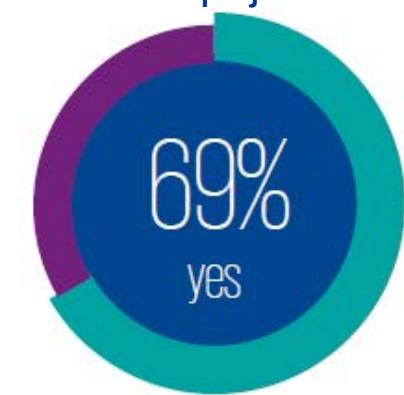
Trgovina



Avtomobilizem



Skupaj



Consumer loss barometer
KPMG

Varnostni napadi v zadnjih 2 letih

Skupaj



Finančna industrija



Tehnologija



Trgovina



Avto industrija



Škodljiva
koda

Interni

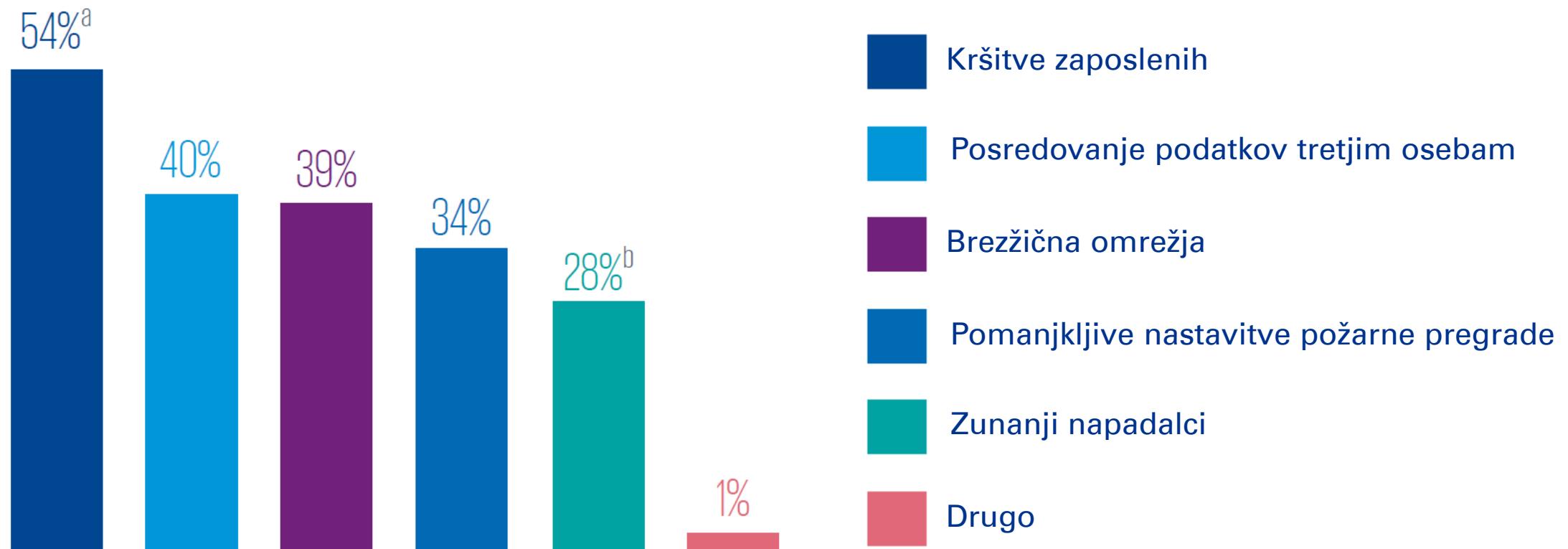
Botnet

Ostalo

Nič

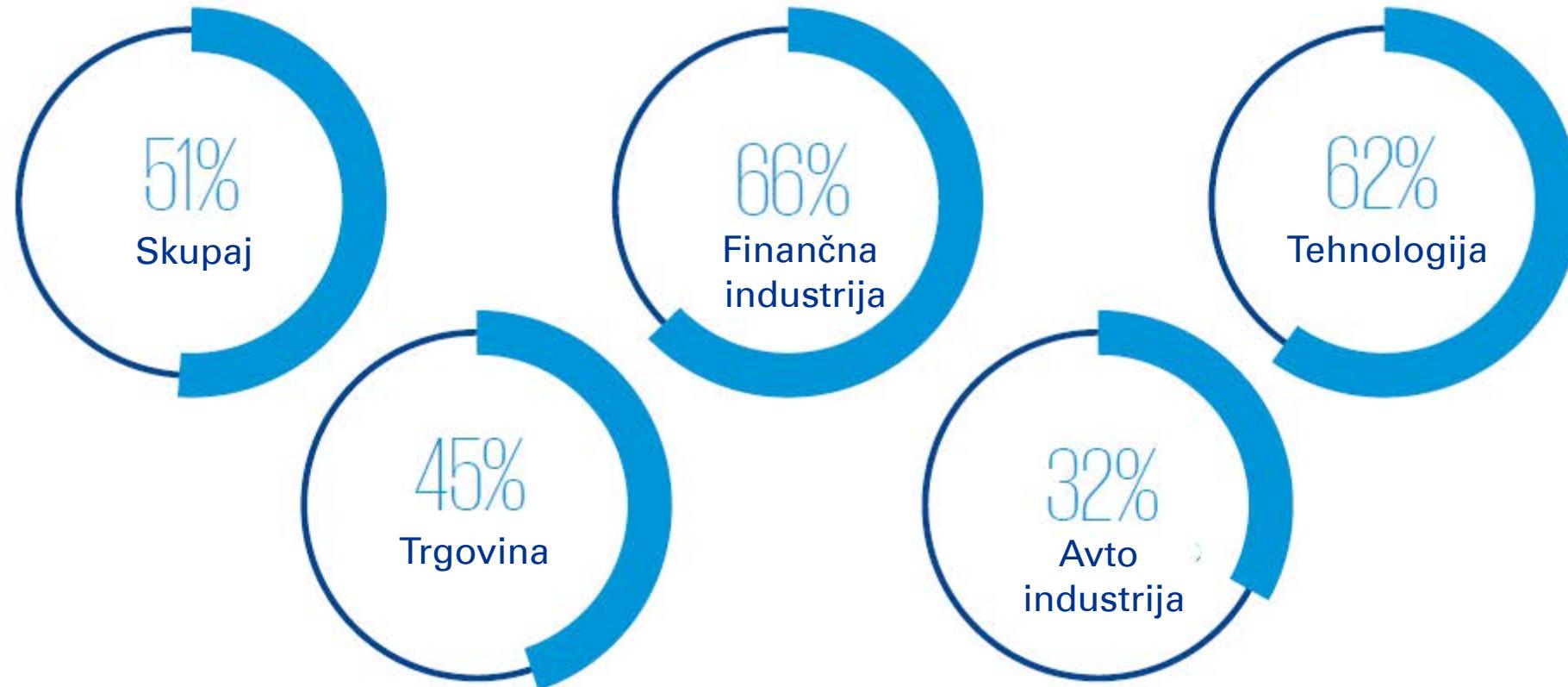
Consumer loss barometer KPMG

Zaposleni so najšibkejši člen kibernetske varnosti



Consumer loss barometer
KPMG

Investicije za zagotavljanje kibernetske varnosti



Consumer loss barometer KPMG

Večja tveganja in stroški

Skupaj



Finančna industrija



Tehnologija



Trgovina



Avto industrija



Ugled

Finančne
izgube

Varnost
zaposlitve

Zakonski
nadzor

Ostalo

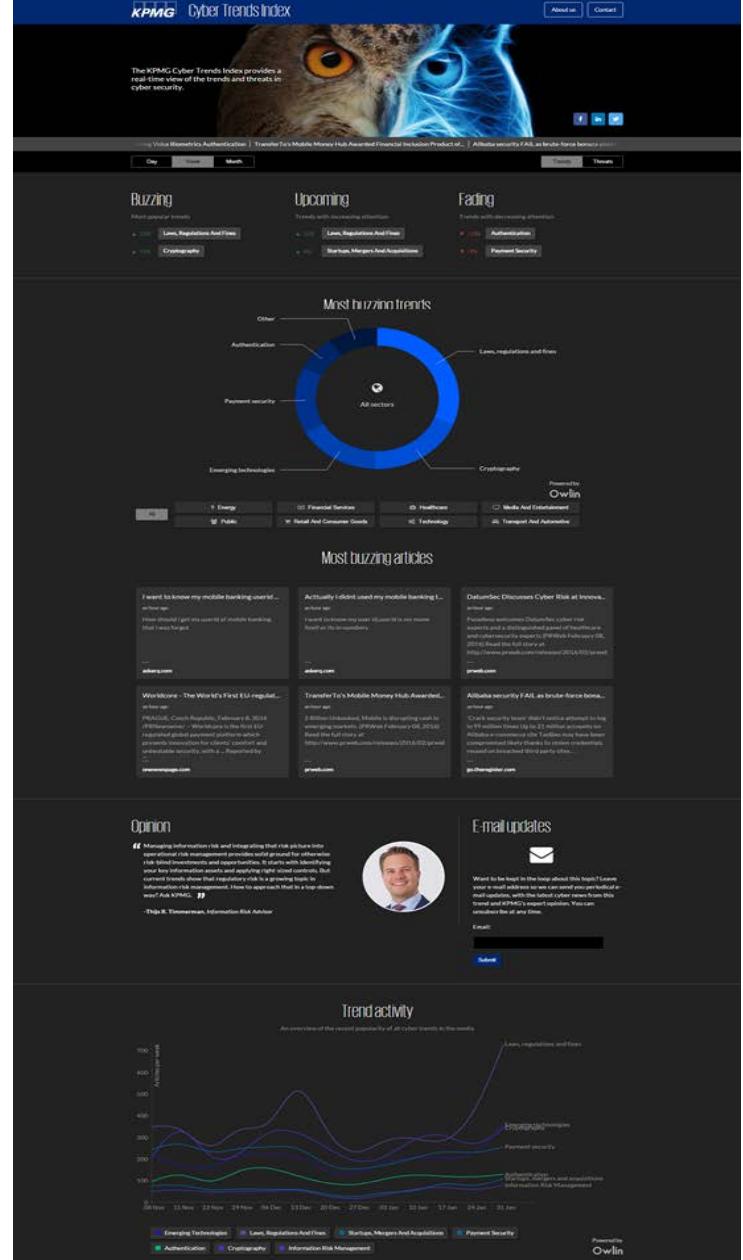
Consumer loss barometer KPMG

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



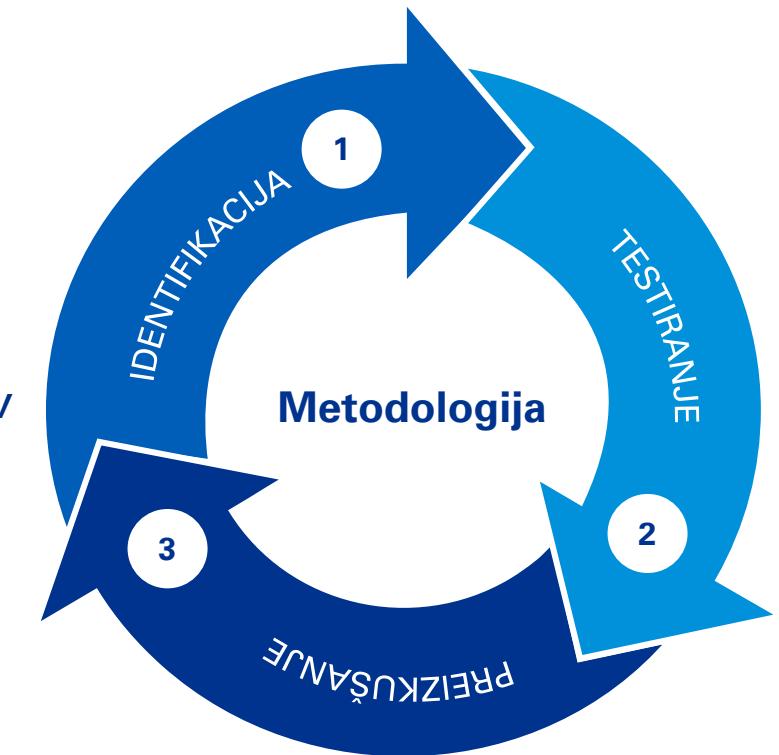
Kibernetska varnost je več kot tehnološki problem!

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

Zakonodaja in standardi

Evropska zakonodaja

Slovenska zakonodaja

Standardi

Dobre prakse





Zakonodaja

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 upravljalcev 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**



© 2016 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.



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



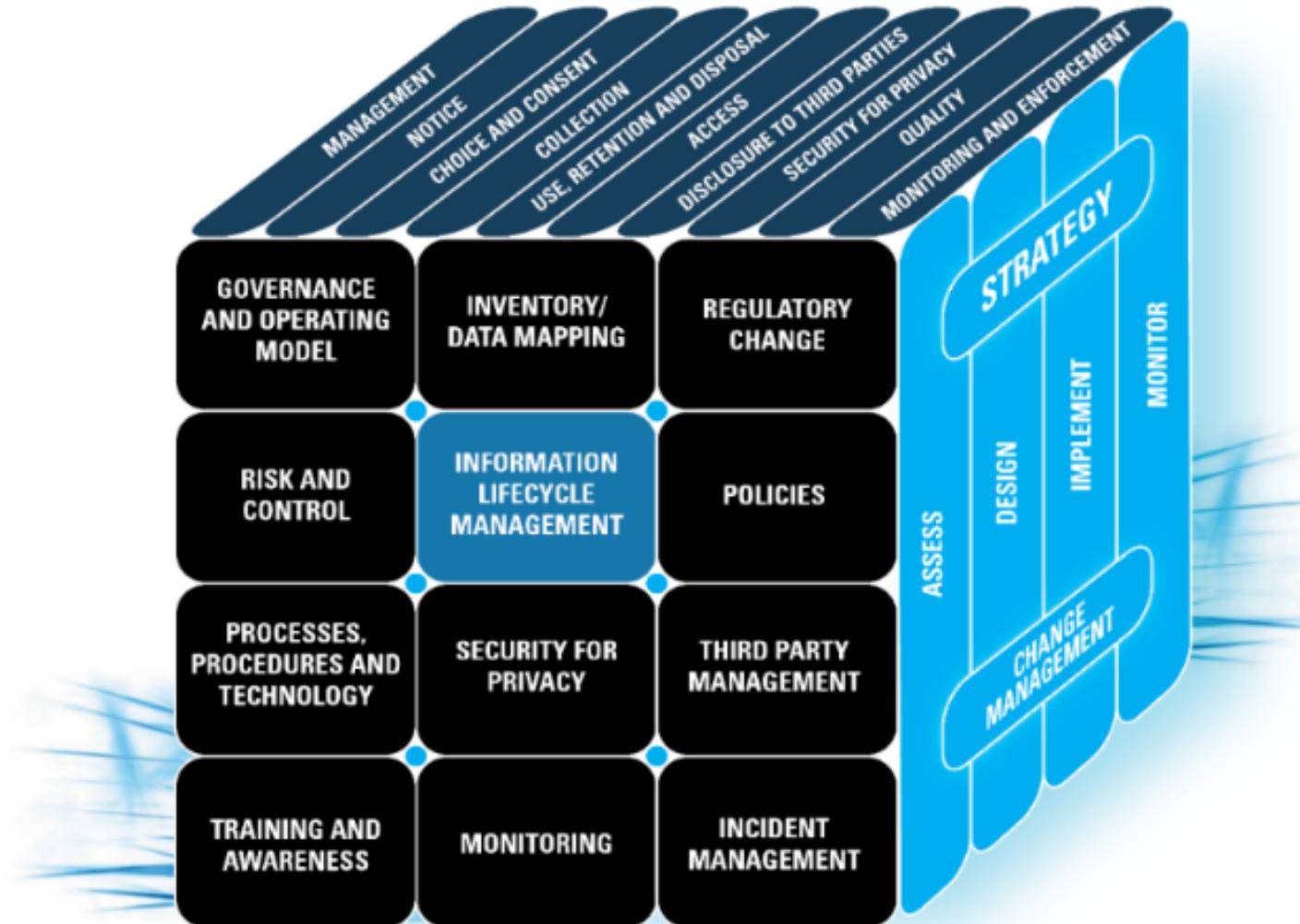
Število pregledov povezanih z varstvom osebnih podatkov se bo zelo povečalo.
Kršitve/kraje osebnih podatkov bodo hitreje javno razkrite.

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.



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



Zmote kibernetiske varnosti



Dosegli bomo 100% varnost

100% varnost ni možna in ni realen cilj.



Nakup najboljše tehnologije nam zagotavlja varnost

Učinkovita kibernetiska varnost je manj odvisna od tehnologije kot si mislimo.



Naše orožje mora biti boljše od napadalcev

Varnostna politika mora zasledovati cilje organizacije in ne ciljev napadalcev.



Za zagotavljanje skladnosti kibernetiske varnosti je dovolj učinkovit nadzor

Zmožnost učenja je enako pomembno kot nadzor.



Zaposlitev najboljših strokovnjakov, bo ustavila kibernetiske nevarnosti

Ključen je pristop, saj kibernetiska varnost ni organizacija.

Razvoj

KPMG Cyber Trends Index

The screenshot shows the homepage of the KPMG Cyber Trends Index. At the top, there is a navigation bar with links to 'DETECTION AGENCY', 'How automated investigation can accelerate threat detection', 'Who is Julian Assange and why is the WikiLeaks founder wanted by Sweden?', 'Ransomware', 'Cyber Threat Intelligence', 'Cyber Risk Intelligence', 'About us', and 'Contact'. Below the navigation bar, there are three tabs: 'Day', 'Week', and 'Month'. On the right side of the header, there are two more tabs: 'Trends' and 'Threats'. The main content area features a large image of a person's hands holding a smartphone. Below the image, there are two news snippets. The first snippet is titled 'Threatpost: Yahoo Tells SEC It Knew About Data Breach in 2014' and includes a short description: 'Yahoo's latest SEC filing includes confirmation that it knew attackers were on its network in 2014 and stole information on 500 million accounts...'. The second snippet is titled 'Adobe fixes flaws in Flash Player and Adobe Connect' and includes a short description: 'Adobe Systems has released scheduled security patches for its widely used Flash Player software as well as the Adobe Connect web conferencing platfor...'. The URL <http://cyber.kpmg.com> is visible at the bottom of the page.

— Pregled objave varnostnih dogodkov v realnem času

— Novice, trendi, nove ranljivosti in rešitve

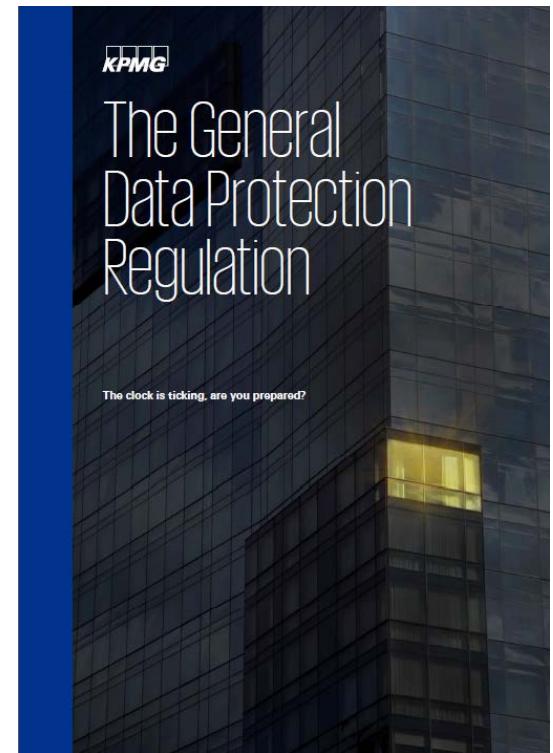
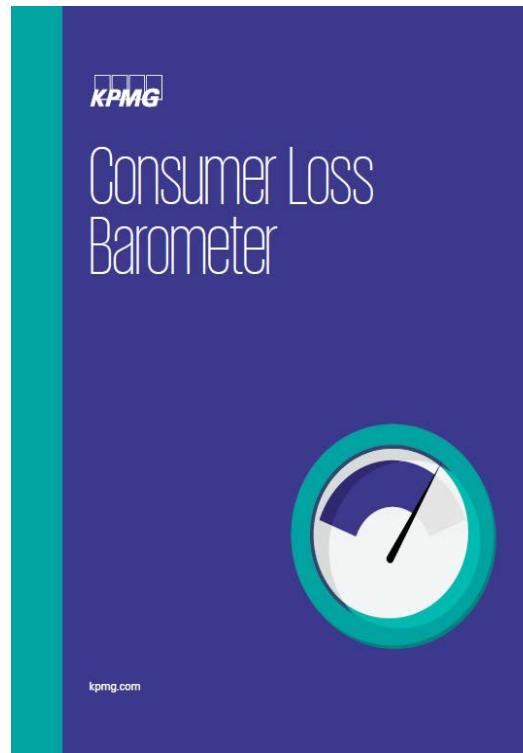
— Spremljanje kibernetskih napadov



Matjaž Pušnik
Manager, IT svetovanje in revizija
KPMG Slovenija

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

kpmg.com



© 2016 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.



Hvala

Matjaž Pušnik

KPMG

matjaz.pusnik@kpmg.si

CISCOSEC