Pri prieskume napríklad zistili veľké rozdiely už len v označovaní miest, ktoré sú snímané kamerami (80 percent v Nórsku oproti len 20 percentám v Maďarsku či Rakúsku).

Každej kamery sa dá zmocniť

V správe Európskej únie sa píše aj o tom, že snímaný človek by mal mať možnosť vedieť, ako a kde sú jeho zábery ukladané. Tento fakt považuje za dôležitý aj expert na počítačovú bezpečnosť Ivan Kopáčik zo spoločnosti Gordias. To už sa však dostávame od verejných priestorov k domácnostiam. Aj v nich máme v súčasnosti mnoho kamier. Na pohľad neškodných, pretože patria nám - sú na našich notebookoch, herných konzolách, mobiloch a iných zariadeniach.

„V princípe by ľudia mali myslieť na to, že všetko, čo sa dá zapnúť oprávneným spôsobom, sa dá zvyčajne zapnúť aj neoprávnene. Vždy je riziko nejakého vírusu alebo škodlivého kódu, ktoré keď si užívateľ spustí, môže sa stať, že kamera sa zapne bez jeho vedomia," hovorí Kopáčik a dodáva, že niektoré škodlivé kódy vedia dokonca znefunkčniť aj LED svetielko, ktoré signalizuje zapnutú kameru, takže ľudia môžu byť naozaj sledovaní bez toho, že by si čokoľvek všimli.

„Ľudia používajú aj mechanické riešenie. Zazrel som človeka, ktorý mal na svojom iPade kameru prelepenú páskou."

Ivan Kopáčik, expert na počítačovú bezpečnosť zo spoločnosti Gordias

Ivan Kopáčik varuje, že akúkoľvek kameru možno aktivovať aj neoprávnene.

Napokon to nie je žiadna hypotetická obava. Pred dvoma rokmi odsúdili hackera Matthewa Andersona na 18 mesiacov za to, že vďaka spamovým emailom získal kontrolu až nad 200-tisíc počítačmi. Neuspokojil sa len s cudzími dátami. Keď polícia zaistila jeho počítač, našla v ňom aj niekoľko videí, na ktorých sa prechádzajú pred svojimi webkamerami nahí ľudia z napadnutých počítačov. „Ako sa chrániť? V prípade počítačov dodržiavať zásady bezpečnosti práce s technikou," tvrdí Kopáčik.

Znamená to mať zapnutý firewall, využívať antivírusové programy, sťahovať si najnovšie bezpečnostné aktualizácie operačných systémov, ale napríklad mať aj riadne zabezpečenú sieť, cez ktorú sa človek pripája na internet. „Všimol som si, že niektorí ľudia používajú aj mechanické riešenie. V kaviarni som napríklad zazrel človeka, ktorý mal na svojom iPade kameru prelepenú páskou. To je vlastne najistejšie riešenie," uzatvára s úsmevom Kopáčik.

Sen marketérov?

Prelepiť si kameru - to môže fungovať pri notebookoch a vari aj tabletoch a mobiloch. Iná elektronika však kameru využíva ako základ svojej funkcionality. Napríklad herné konzoly ovládané pohybom človeka pred kamerou. Prípadne inteligentné televízory, ktoré kamery využívajú na rozpoznávanie členov domácnosti a následné upravenie nastavení. Práve tieto zariadenia sa v posledných mesiacoch stali terčom slovných útokov v súvislosti s obavami o súkromie.

Nečudo, veď hackerský útok na kameru v počítači je síce možný, ale málo pravdepodobný. Pokiaľ nie ste celebrita, zábery na vaše nahé telo určite pre hacerka nemajú veľkú hodnotu. Útoky s motívom vydierania sú tiež len ojedinelým javom. Kamery v televízoroch a herných