HOTEL / RESTAURACE / KAVÁRNA / BAR / CATERING

HOREKA MAG

horekaweb.cz: 100% spojuje!

#107
01-02/2018

2318

SDÍLEJTE INFORMACE,
ZAPOJTE SE DO DISKUSE,
INSPIRUJTE SE A BAVTE SE!

JAKÁ BY MĚLA BÝT KAVÁRNA 21. STOLETÍ? STR. 20

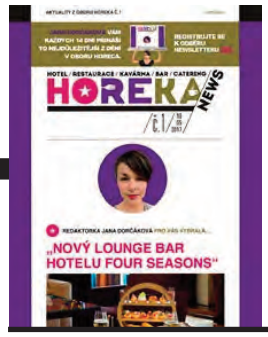
REGISTRUJTE SE K ODBĚRU NEWSLETTERU!

JANA DORČÁKOVÁ
JANA.DORCAKOVA@ATOZ.CZ
/EHOREKA

HACKERSKÝ ÚTOK SE TÝKÁ I VÁS

V dnešním světě musí hoteliér myslet na ochranu svého podnikání a hostů i ve virtuálním prostoru. Karol Suchánek, odborník na cyber security, pro vás vybral pár tipů, jak na to.

KAŽDÉ DVA TÝDNY NEWSLETTER PLNÝ NOVINEK



Googlili jste si někdy své jméno? Pokud ne, zkuste to, budete překvapeni, jakou stopu jste ve virtuálním světě zanechali. On-line prostředí je přeplněno nejenom zábavným obsahem, ale i tipy, jak získat přístup k háklivým údajům.

AŤ MAJÍ HOSTÉ JEDINEČNÁ HESLA PRO WI-FI

Začneme úplnými základy. „Velký problém jsou otevřené wi-fi sítě,“ upozorňuje Karol Suchánek. „Je to bezpečnostní riziko hlavně pro hosty, ne až tak pro hoteliéra. Pokud jsou na veřejnou wi-fi připojené i podnikové přístroje, tak je to opravdu špatně. Útočník se může do sítě dostat, zjišťovat, kdo navštěvuje jaké stránky, kam se přihlašuje, anebo udělat tzv. SSL strip, což je dešifrování chráněného prostředí, díky čemuž odchytí přihlašovací údaje.“

Dnes už nemusíte být ani zkušený hacker, na YouTube existuje tisíc návodů, jak hacknout veřejnou wi-fi síť. „Zlatým standardem je proto mít wi-fi pod heslem, které má každý host jedinečné, generuje se například od čísla pokoje a jeho příjmení,“ radí Karol Suchánek. Dále je oblíbený tzv. hotel hacking. Útočník přijde do hotelu a hackuje hosty. Mnozí dokážou vyrobit falešné wi-fi sítě, na které se hosté připojují a myslí si, že je to oficiální hotelová síť.

Pokud chcete přijít na to, co by mohlo být v hotelu lepší z kybernetického hlediska, Karol Suchánek doporučuje najmout si tzv. white hats hackers, tudíž profesionály, kteří jsou na dobré straně a odhalují díry v systému. Cena závisí na tom, co všechno si dáte otestovat, tato služba je zcela běžná a dostupná i v České republice. „Kontroly je ale nutné dělat pravidelně, alespoň jednou za rok, protože se technologie každým dnem vyvíjí.“

MĚJTE JASNĚ STANOVENÉ KROKY

Určitě je mít dobré i plán v případě ohrožení technologií v hotelu. Například když se porouchá klimatizace v serverovně.

Třeba si myslíte, že vám nic nehrozí. Omyl. „Například vám může hacker zablokovat vstupní karty, zašifrovat systémy a pak se už nikdo nedostane do pokojů.“

Nezapomínejte také na pravidelné školení personálu. „Pokud přijde někdo z ulice, že ztratil kartu od pokoje, personál ho musí identifikovat a nevystavit kartu někomu jenom tak,“ upozorňuje Karol Suchánek, který takhle testuje hotely, v nichž je ubytovaný. Většinou mu kartu vydají bez jakékoliv kontroly. Nikdy nesmí nikoho cizího pouštět do vaší serverovny atd. Zkrátka stanovit si jasné procedury. „Také doporučuji nastavit pravidla pro používání například USB zařízení vašich zaměstnanců.“

Nikomu se nechce ani pomyslet na možný kybernetický útok. Když už náhodou přijde, je dobré být připraven. ◆

Kdo je Karol Suchánek?

Informační technologie jsou pro Karola Suchánka koníčkem už od střední školy. Bezpečnostní software, který vyvinul v šestnácti letech, nakonec vyhrál středoškolskou soutěž a dostal se až do běžného prodeje. První část profesionální kariéry pracoval na vývoji softwaru a získal titul bakaláře informačních technologií na Univerzitě Konštantína Filozofa v Nitře a později také MBA na University of New York in Prague. Jeho zájem o technologie ho přivedl k problematice cybersecurity, o které dnes přednáší a organizuje semináře pro širokou veřejnost. Pro firmy pak organizuje cybersecurity koučink pro klíčové zaměstnance a jejich rodinné příslušníky. Je absolventem speciálního cybersecurity programu na Massachusetts Institute of Technology (MIT) v Bostonu.

Otestujte si jednoduše svůj „backup plan“

- v pondělí si vytvořte soubor
- v úterý soubor smažte
- ve středu běžte za vaším IT zaměstnancem, ať vám ho obnoví

Pokud ho obnoví, vše funguje, jak má!