

# STAVEBNÍ FIRMY ČELÍ HACKERSKÝM ÚTOKŮM. KDE ZAČÍT S OBRANOU?

12.2.2025 - Denisa Kolaříková, Tereza Štosová | Crest Communications/PLANRADAR ČR

**Kybernetické útoky, jako je phishing, ransomware nebo útoky na zálohované soubory, jsou v současnosti stále častější.**

*„Zabezpečení citlivých údajů je s rostoucí digitalizací ve stavebním sektoru naprosto zásadní pro úspěšné fungování firem. Kybernetická bezpečnost přitom nespočívá pouze v kvalitních technologiích, ale především v prevenci, vzdělávání a vytváření správných bezpečnostních návyků u vlastních zaměstnanců. Bez těchto opatření může i drobná lidská chyba způsobit vážné narušení projektů a ztrátu důvěry klientů,“* vysvětluje **Adam Heres Vostárek, regionální manažer PlanRadaru pro Českou republiku.**

## Alarmující nárůst kyberútoků

Kybernetické útoky, jako je phishing, ransomware nebo útoky na zálohované soubory, jsou v současnosti stále častější. Podle mezinárodní analýzy z roku 2024[1], která proběhla ve 14 zemích světa, zažila naprostá většina stavebních a realitních společností (enormních 96 %) kybernetické útoky, které zahrnovaly pokus o poškození zálohovaných dat, přičemž 61 % těchto pokusů bylo úspěšných. Tyto útoky mají přitom dalekosáhlé důsledky – od finančních ztrát přes narušení provozu až po poškození pověsti firmy. Situace tak ukazuje na nezbytnou nutnost posílit kybernetickou bezpečnosti v rámci celého odvětví.

## Jak předejít napadením?

Aby se firmy mohly těmto hrozbám účinně bránit, je třeba zavést několik klíčových opatření. Jedním z nich je vícefázové ověřování, které přidává další vrstvu ochrany nad rámec běžných hesel. Dalším důležitým krokem je omezení přístupových práv. To znamená, že konkrétní zaměstnanci by měli mít přístup pouze k těm informacím, které jsou nezbytné pro výkon jejich práce, a ne k datům za celou společnost. Moderní softwarové platformy, jako je PlanRadar, umožňují tyto procesy efektivně řídit, a navíc nabízejí možnost monitorování aktivit uživatelů či šifrování dat.

Neméně důležité je pravidelné zálohování dat a vytvoření plánu obnovy pro případ, že by firma čelila útoku. Kombinace lokálních a cloudových úložišť zvyšuje úroveň ochrany a umožňuje rychlejší zotavení z případných incidentů. Důraz by měl být kladen i na pravidelné aktualizace softwaru, které zajišťují ochranu před nově objevenými zranitelnými místy.

## Lidský faktor jako klíčový bezpečnostní prvek

Kromě důsledného zálohování však hraje významnou roli chování zaměstnanců. Další globální průzkum z roku 2024[2] ukazuje, že přibližně jedna čtvrtina organizací (25,7 %) nezajišťuje svým pracovníkům pravidelné školení v oblasti IT bezpečnosti. Tento zásadní nedostatek ve vzdělávání představuje kritický bezpečnostní problém, a to zejména u menších společností. Ve stavebnictví, kde jedna lidská chyba může znamenat neoprávněný přístup k širokému spektru dat a informací od řady spolupracujících subjektů, je vzdělávání vlastních zaměstnanců v oblasti kybernetické bezpečnosti nezbytné. Pravidelná školení, která vedou k rozpoznávání hrozeb a správnému nakládání s daty, jsou tudíž při snižování rizika kybernetických útoků naprosto zásadní.

## Ochrana dat je nezbytností moderní doby

*„Kyberbezpečnost ve stavebnictví vyžaduje komplexní přístup, který propojuje moderní technologie s prevencí a vzděláváním zaměstnanců. Správným nastavením bezpečnostních opatření mohou stavební firmy nejen minimalizovat riziko úniku citlivých informací, ale také lépe čelit rostoucím požadavkům digitalizace,“ komentuje Adam Heres Vostárek. Tento přístup firmám umožňuje optimalizovat jejich provoz, udržovat si důvěru svých partnerů a klientů a současně se připravit na budoucí výzvy v tomto dynamicky se rozvíjejícím odvětví. Ochrana dat již není pouhou otázkou prevence, ale zásadním krokem k zajištění dlouhodobé stability a konkurenceschopnosti.*

### **Pro více informací kontaktujte:**

Crest Communications, a.s.

Denisa Kolaříková

Account Manager

Gsm: +420 731 613 606

E-mail: [denisa.kolarikova@crestcom.cz](mailto:denisa.kolarikova@crestcom.cz)

[www.crestcom.cz](http://www.crestcom.cz)

Tereza Štosová

Account Executive

Gsm: +420 778 495 239

E-mail: [tereza.stosova@crestcom.cz](mailto:tereza.stosova@crestcom.cz)

### **O PlanRadaru**

PlanRadar je oceňovaná digitální platforma na bázi SaaS (z anglického “Software as a Service”) pro dokumentaci, komunikaci a reporting během výstavby a správy nemovitostí. Platforma funguje po celém světě, v současnosti na více než 75 trzích. PlanRadar zjednodušuje každodenní procesy a komunikaci v uživatelsky přátelské digitální platformě, která propojuje všechny zúčastněné strany na projektu a poskytuje přístup k relevantním informacím v reálném čase. Zákazníkům umožňuje pracovat efektivněji a dosahovat vyšší kvality i transparentnosti. Platforma je přínosná pro každého člověka zapojeného na projektu, od stavbyvedoucích přes architekty a projektové manažery až po vlastníky. Navíc je vhodná pro společnosti různého typu zaměření i velikosti. V současnosti PlanRadar používá více než 170 000 profesionálů ke sledování, sdílení a řešení problémů, ať už přímo na místě anebo připojením na dálku. Aktuálně je k dispozici ve více než 25 jazycích a lze jej používat na všech zařízeních iOS, Windows a Android. Společnost PlanRadar se sídlem ve Vídni v Rakousku má 13 poboček po celém světě. Více o společnosti se dozvíte na <https://www.planradar.com/cz/>.

[1] Zdroj: [sophos-state-of-ransomware-2024-wp.pdf](#). Analýza probíhala ve vybraných státech v regionu EMEA, Americe, Asii a Tichomoří.

[2] Zdroj: <https://www.hornetsecurity.com/en/blog/security-awareness-survey-2024/>

<https://www.crestcom.cz/cz/tiskova-zprava?id=5409>