5 tipů, jak hned začít s kyberbezpečností

1 Aktualizujte

Veškerý firemní software i systémy udržujte aktualizované. Z průzkumu společnosti Verizon s názvem Data Breach Investigations Report z roku 2021 například vyplývá, že 60 % útoků se dalo zabránit právě aktualizací softwaru. Je to jeden z kroků, jejichž pomocí se dá předejít celé paletě hrozeb, a můžete ho ve firmě zavést poměrně rychle. Abyste na aktualizace nezapomínali, nastavte si automatické aktualizace.

2 Ověřujte

Zaveďte dvoufaktorové ověřování. Používat při přihlašování pouze jméno a heslo je zastaralý koncept. Pro vstup do systémů, ve kterých pracujete, proto vyžadujte více než jedno potvrzení identity. Není to sice všespásné řešení, ale je to jeden z účinných kroků, jak začít. Zapomeňte na SMS, zajistěte si autentizační mobilní aplikaci nebo bezpečnější hardwarové tokeny.

3 Zálohujte

Cílem velké části kybernetických útoků je ukrást firmě data a následně jí je prodat zpět. Data vaší firmy a vašich klientů mají cenu zlata. Přijít o ně by vás stálo nejen ztrátu zákazníků, ale také ztrátu reputace. A tu máte jenom jednu. Zálohujte proto správně, ať o data ani reputaci nepřijdete. Obecně doporučujeme zálohovat 1× denně a minimálně 1× týdně by měla proběhnout kompletní záloha dat. Samozřejmě záleží na důležitosti dat pro chod firmy. Je tedy pravděpodobné, že data z různých systémů se budou zálohovat s různou frekvencí.

Při zálohování se řiďte pravidlem 3–2–1. To ve stručnosti říká, že data by měla být uložená ve 3 kopiích, na 2 různých médiích a minimálně 1 z nich fyzicky mimo pracoviště. Nezapomínejte také na to, že pokud si firemní data zálohujete sami, pravidelně testujte, zdali jste schopni data ze zálohy obnovit.

4 Hesla zodpovědně

Bez jména a hesla se při jakémkoli přihlašování neobejdete. Zajistěte proto, aby vaši zaměstnanci používali dostatečně silná hesla kombinující několik typů znaků a nepoužívali všude stejné. Ideální je mít ke každé službě jiné. Negenerujte ale „silná“ hesla na neznámých stránkách. Nikdy totiž nevíte, kdo se za stránkou schovává. Pokud využíváte správce hesel, pátrejte napřed po pověsti provozovatele. Správce hesel by měl být také dvoufaktorově zabezpečený. Máte rádi správce hesel v prohlížečích? Vyhněte se jim. Riziko zneužití je až příliš velké.

5 Vzdělávejte

Vzdělávejte svoje zaměstnance. Zaměstnanci jsou nejslabším článkem každého kyberbezpečnostního řetězce. Někdy se jim přezdívá „vstupní branou do firmy“. Ku příkladu na odkaz v podvodném e-mailu klikne až 40 % z nich. Investujte proto do školení, vyplatí se.