Newsletter
Únor 2024

Témata

LEXNOVA

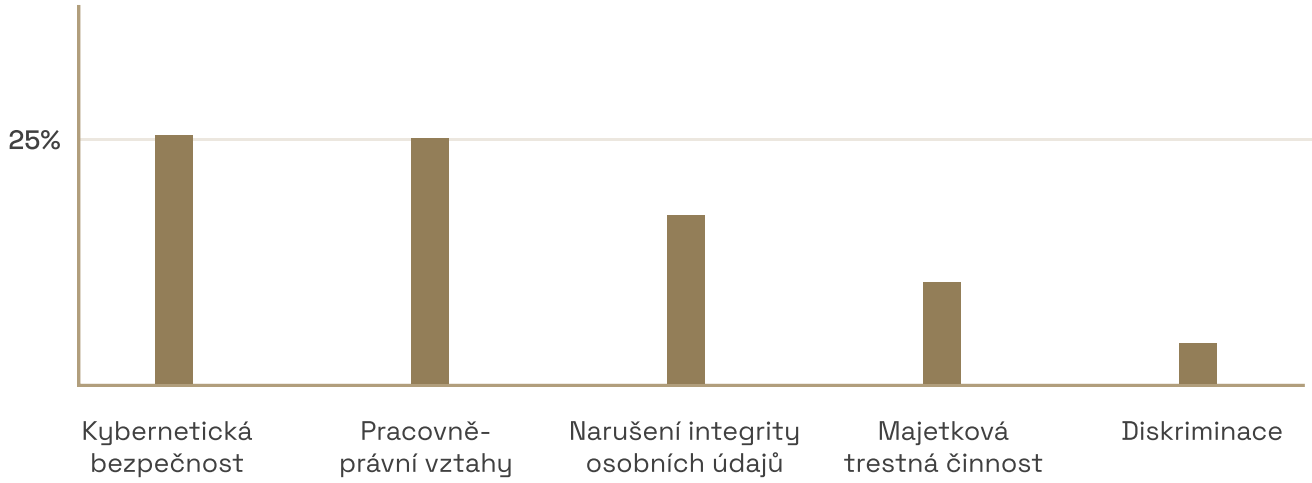
Ochrana oznamovatelů

Je tomu již půl roku, co vešel v účinnost zákon č. 171/2023 Sb., o ochraně oznamovatelů.

Na počátku roku 2024 **Státní úřad inspekce práce plánuje plošné celorepublikové kontroly** způsobu implementace a fungování vnitřních oznamovacích systému u zaměstnavatelů. Proto bychom Vás rádi upozornili na nejčastější chyby, které jsme identifikovali v rámci našeho průzkumu trhu.

V první části průzkum identifikoval oblasti, ve kterých zaměstnanci nejčastěji podávají oznámení.

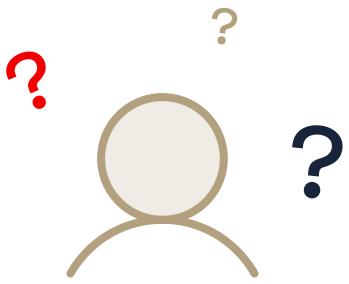
Na děleném prvním místě se umístilo **porušení kybernetické bezpečnosti a spory v oblasti pracovně právních vztahů**. S kybernetickou bezpečností souvisí další časté oznámení týkající se **narušení integrity osobních údajů**. Mezi nejčastějšími oznámeními se také umístila ta, která se týkají **majetkové trestné činnosti a diskriminace.**



Neváhejte nás kontaktovat +420 737 328 987 info@lexnova.cz Lexnova.cz

LEXNOVA

Další důležité zjištění, které průzkum identifikoval, je **nedostatečné informování zaměstnanců** o existenci vnitřního oznamovacího systému.

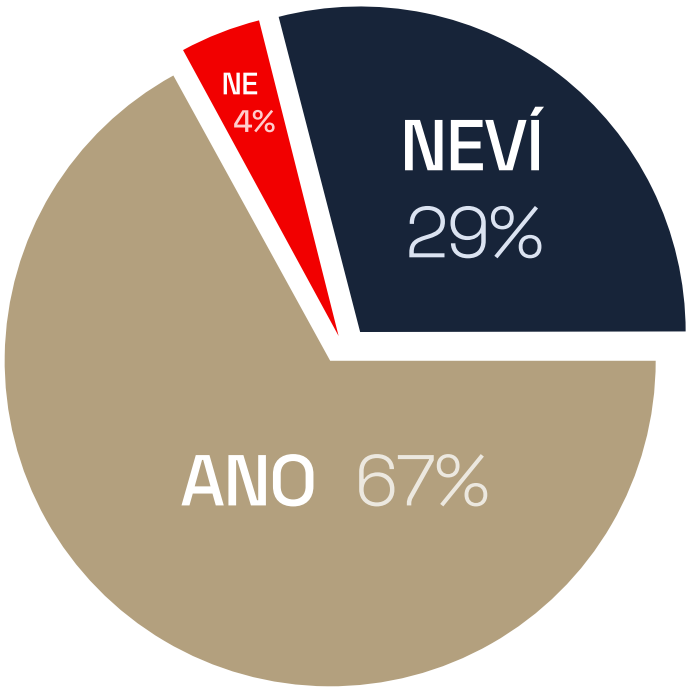


Přestože zákon ukládá zaměstnavatelům povinnost zřídit vnitřní oznamovací systém, většina zaměstnanců o jejich existence neví.

Zajímavé je, že téměř **67 % respondentů je připraveno upozornit** na nekalá jednání.

Zatímco pouze **4 % by se rozhodlo mlčet**.

Ovšem **29 % respondentů neví**, jestli by na nekalé či nezákonné jednání upozornilo.

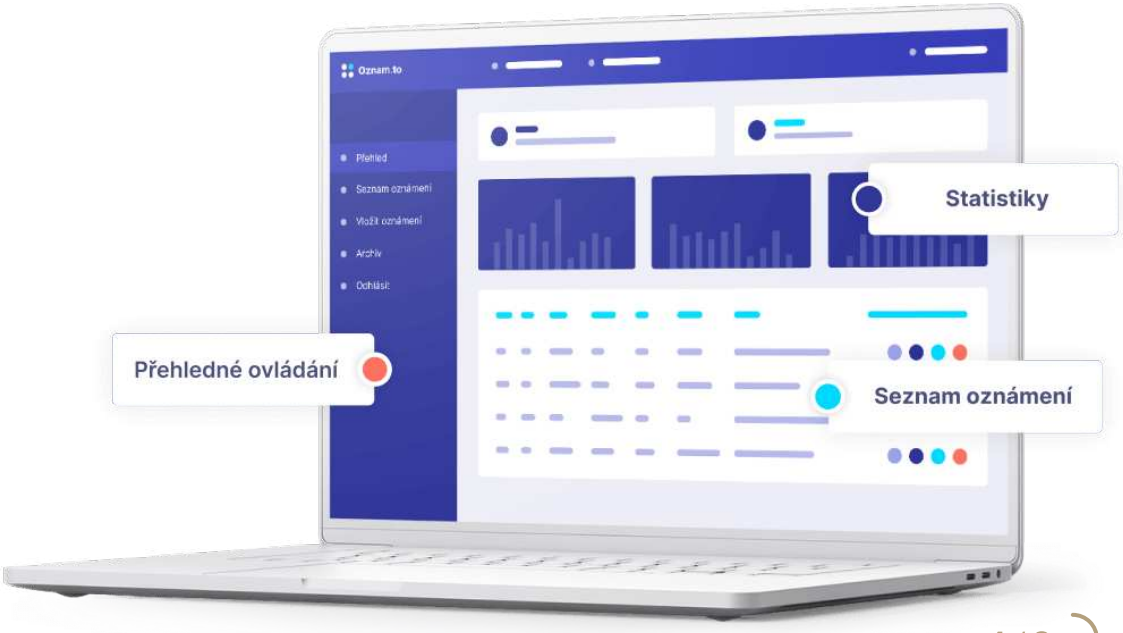


Hlavním faktorem ovlivňujícím tuto nejistotu je **strach** z odvetných opatření, který vyjádřilo až **73 % zaměstnanců**.

Edukace zaměstnanců o existenci a využití vnitřních oznamovacích kanálů se zdá být **nezbytná**.

Podle realizovaného průzkumu byla většina zaměstnanců informována elektronicky, nebo na interních školení. Z výzkumu však vyplývá, že je **žádoucí školení opakovat** v pravidelných intervalech.

Výše popsaná zjištění zdůrazňují důležitost **posílení informačního povědomí a důvěry vůči oznamovacím systémům**, které představují důležitý prvek v boji proti protiprávnímu jednání.



Výsledky

našeho šetření korespondují s tím, na co se Státní úřad inspekce práce plánuje zaměřit.

Chystá se zaměřit nejen na následující oblasti:

- ☑ Zda jsou webových stránkách organizace **zveřejněné zákonné informace**.
- ☑ Jak je zajištěna **nestrannost Příslušné osoby** při případném šetření podnětu oznamovatele?
- ☑ Jak je zajištěno bezpečné **předání oznámení** do rukou Příslušné osoby?
- ☑ Jaké **podmínky** má vytvořené Příslušná osoba pro případná šetření?
- ☑ **Způsob informování zaměstnanců** o jejich právech v souvislosti s tímto zákonem?

Všem klientům, kterým **zajišťujeme roli příslušné osoby** budeme v následujících dnech a týdnech volat a domlouvat si termín kontrolní schůzky.

Budeme rádi, pokud se nám **sami ozvete** s vhodným termínem kontrolní schůzky nastavení prostředí ochrany oznamovatelů.

Miroslav Kvapil, MSc.
spoluzakladatel Lexnova s.r.o.

Jsou si Vaši zaměstnanci dostatečně vědomi rizika Phishingových útoků?

VÝHODNÁ NABÍDKA

Jedno z nejčastějších oznámení od klientů Oznam.to se týká **prolomení zabezpečení hesel** ve firmě či organizaci a s tím související přestupky či trestné činy v podobě krádeže osobních či firemních údajů a dat.

Proto jsme se rozhodli našim klientům nabídnout za **zvýhodněných podmínek profesionální phishingovou kampaň**, která Vám pomůže lépe pochopit, jak Vaši zaměstnanci reagují na škodlivé e-maily a odkazy – pro tentokrát však pouze na zkoušku.

Tato kampaň je jedním z nástrojů, které Vám pomohou identifikovat slabá místa ve Vaší kyberbezpečnosti a posílit Vaše obranné mechanismy.

Výsledky phishingové kampaně tvoří i velmi cenný vstup do auditu, který budete muset realizovat v návaznosti na novou směrnici **NIS2**, respektive připravovaný zákon o kybernetické bezpečnosti. O tomto tématu Vás Budeme detailně informovat v dalším Newsletteru.

NAŠE AKČNÍ CENA
2990 Kč

Neváhejte nás kontaktovat +420 737 328 987 info@lexnova.cz Lexnova.cz

LEXNOVA

Co je Phishingová kampaň?

Realistický simulovaný útok:

Nabídka simulovaného phishingového útoku Vám umožní vidět, jak Vaši zaměstnanci reagují na škodlivé e-maily a odkazy. Tímto způsobem Vám **pomůžeme identifikovat slabá místa** ve Vaší bezpečnosti.

Tréning / školení zaměstnanců:

Máme pro Vaše zaměstnance připraveny tréningy a školení, které přesně a individualizovaně reagují na chyby, které zaměstnanci udělali při simulovaném útoku.

Nejedná se o nudné prezentace, ale **školení je formou her**, interaktivních testů či formou speciálního seriálu.

Naše školení má reálný dopad a **snižuje škodlivé chování zaměstnanců** v online světě o 90 % během několika měsíců.

↘ 90 %

Pokud máte zájem o **profesionální phishingovou kampaň**, kontaktujte nás. Budeme rádi, pokud nás v této věci propojíte s Vaším IT manažerem.

Příště

V příštím newsletteru se budeme
věnovat následujícím tématům.

Pokud byste byli nedočkaví, zavolejte nám.
Rádi si s Vámi domluvíme osobní schůzku
a probereme vše potřebné u kávy.

Nové trendy a zákony sledujeme za Vás.

Příští témata

ESG

NIS2

Sdílená energetika

**Administrativně nenáročné dotace na IT
či technické vzdělávání zaměstnanců
se spoluúčastí zaměstnavatele pouze 5 %**

Neváhejte nás kontaktovat

+420 737 328 987

info@lexnova.cz

www.lexnova.cz

LEXNOVA