

Дії, які організації мають вживати, коли виявлено порушення безпеки

Повідомте про проблему

Спілкування створює прозорість, що дуже важливо в таких ситуаціях.

Внутрішньо всі співробітники повинні бути поінформовані і чітко озвучений план дій.

З зовнішніми клієнтами необхідно зв'язатися безпосередньо, а також потрібно зробити офіційне повідомлення.

Будьте щирими та визнайте свою відповідальність

Відповідайте на порушення чесно і щиро, беручи відповідальність за вину організації.

Надайте детальну інформацію

Поясніть, чому ситуація відбулася і що конкретно було скомпрометовано. Загалом очікується, що організації оплачуватимуть будь-які витрати клієнтів, пов'язані з подіями крадіжки особистих даних, що сталися в результаті порушення безпеки.

Знайдіть причину

Вживайте заходів, щоб зрозуміти, що спричинило та сприяло порушення. Це може передбачати найм експертів-криміналістів для дослідження та з'ясування деталей.

Врахуйте отриманий досвід

Переконайтеся, що всі уроки, отримані під час розслідувань, враховані, щоб запобігти подібним порушенням у майбутньому.

Перевірте, а потім перевірте ще раз

Зловмисники часто намагаються залишити чорні ходи для полегшення майбутніх втручань. Щоб цього не сталося, переконайтеся, що всі системи чисті, не встановлені бекдори та нічого іншого не було зламано.

Навчайте

Підвищуйте обізнаність, тренуйте та навчайте співробітників, партнерів і клієнтів, як запобігти майбутнім порушенням.

From:
<https://wiki.djal.in/> - IT - wiki

Permanent link:
https://wiki.djal.in/doku.php/security/checklist/diji_jaki_organizaciji_majut_vzhivati_koli_vijavleno_porushennja_bezpeki

Last update: **2023/09/24 05:10**

