ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС АД

Ние не следваме, а изпреварваме събитията!

ВАШЕТО СПОКОЙСТВИЕ И ЗАЩИТА СА НАША РАБОТА

Ние сме застрахователна компания от ново поколение, която комбинира последните технологии в киберсигурността с експертни застрахователни решения, предоставяйки ви активната сигурност и спокойствието, от които се нуждаете в дигиталния свят.

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

Имаме кибер решение, създадено за нуждите на адвокати, адвокатски дружества, нотариуси и частни съдебни изпълнители

ЗАЩО Е НУЖНО ДА ПОМИСЛИТЕ?

Ние знаем, че вашият бизнес се дигитализира успешно, за да направи работата ви бърза и качествена. Но знаете ли, че този процес крие рискове в изтичане на данни и увреждане на компютърните системи? Знаете ли, че можете да станете мишена на кибер изнудване?

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

ЗАЩО ДА ОБЪРНЕТЕ ВНИМАНИЕ?

Кибер престъпленията не се случват само на крупни корпорации, банки и публични институции. В действителност, малките и средноголемите компании често са на прицел, защото са по-уязвими и не подозират дигиталната заплаха. Дори и бизнесът да се представлява само от един човек, той също е в опасност, защото използва всякакви дигитални устройства - компютър, таблет, телефон.

Вие сте адвокат, нотариус или частен съдебен изпълнител?

Трябва да знаете, че е възможно да сте под заплаха. От доклада за киберсигурност на ABA, става ясно, че **25% от адвокатските кантори са претърпели нарушение на данните. Това се случва все по-често и заплашва както поверителността на чувствителната информация на клиентите ви, така и репутацията на фирмата ви.** Докладът показва, че киберсигурността трябва да бъде постоянен приоритет за адвокатските кантори, които имат задължението да защитават информацията на своите клиенти.

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

КАКВИ СА КИБЕРПРЕСТЪПЛЕНИЯТА?

Унищожаване, повреждане, кражба на информация

52 млрд. долара са загубите през 2022 г., свързани с откраднатата самоличност онлайн - при това само в САЩ. Данните на общо 42 млн. американски граждани са били ползвани неправомерно през последната година, сочат данни на Javelin Strategy & Research.

Заплаха за извличане на информация от Дигитални активи

4.35 млн. долара е средният разход на компания след изтичане на данни, сочат данните на IBM. Това обхваща предимно големи компании, които работят с данни на милиони клиенти. Най-тежки са изтичанията на данни от компании в сферата на здравеопазването, където средният разход е 10.1 млн. долара.

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

ХАКЕРСКИ АТАКИ

45% от компаниите глобално ще бъдат засегнати от киберинцидент, свързан с веригата им на доставки, в периода до 2025 г., сочи анализ на анализаторската компания Gartner.

Заплаха за ограничаване и възпрепятстване на достъпа до компютърните системи

18 хил. долара струва средно на една американска фирма каквато и да било кибератака - изтичане на данни, рансъмуер или DDoS. Данните са за 2022 г., като скокът е с около 50% спрямо 2021 г., сочи докладът Hiscox Cyber Readiness, според който 47% от всички американски бизнеси са имали проблем с киберзащитата си през последната година.

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

Нарушаване неприкосновеността и причиняване неизправност в дигиталните активи

2.5 терабита в секунда е най-голямата засечена DDoS атака през 2022 г. според данните на **Cloudflare**. DDoS (Distributed denial of service) атаките представляват генериране на фалшив трафик, който да попречи на истински потребители да достъпят даден сайт или услуга.

61% е повишението на броя на фишинг атаките през 2022 г. според доклада State of Phishing на **SlashNext**. Само през третото тримесечие на годината е имало 3 млн. различни видове фишинг атаки, най-голямата регистрирана активност до този момент от организацията.

Кражба на потребителски достъпи и банкови индентификации

65 хил. софтуерни пробойни са били открити само през 2022 г. от етични хакери. Числото е с 21% по-високо спрямо година по-рано, сочат данните от доклада Hacker Powered Security.

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

ЗАЩО ДА СЕ ЗАСТРАХОВАТЕ С НАС?

Нашите кибер решения са разработени съвместно с едни от най-признатите експерти в сферата на киберсигурността в света. **Ние сме на разположение 24/7, предоставяйки ви 3 нива на реакция.** Не на последно място, ние ви презастраховаме за стойността на пълното покритие на вашите загуби/разходи, според условията на вашата полица. Наш презастрахователен партньор е третият по големина в света презастраховател - Hannover Re.

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

НАШИТЕ КОМПЛЕКСНИ КИБЕР РЕШЕНИЯ:

Обучения от Cyber 360 Academy

Академията предоставя програми за обучение, ръководени от топ експерти в индустрията, с дългогодишен опит. При успешно завършване, всеки курсист получава официален сертификат.

Техническа поддръжка от Cyber One

Бизнесът ви се възползва от ефективен инструмент за анализ на риска - нашият SOC. С ранна реакция системата за мониторинг SIEM разпознава неоторизираните действия в мрежата ви преди те да успеят да ви навредят. Чрез нашата незабавна обратна връзка получавате три нива на съдействие чрез нашата гореща линия.

Кибер застраховане от Лев Инс

Предоставяме ви цялостни решения за киберсигурност, с индивидуално предложение за покрити рискове и специални цени, съобразени с размера и нуждите на конкретната организация.

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ ЛЕВ ИНС АКТИВНАТА СИГУРНОСТ

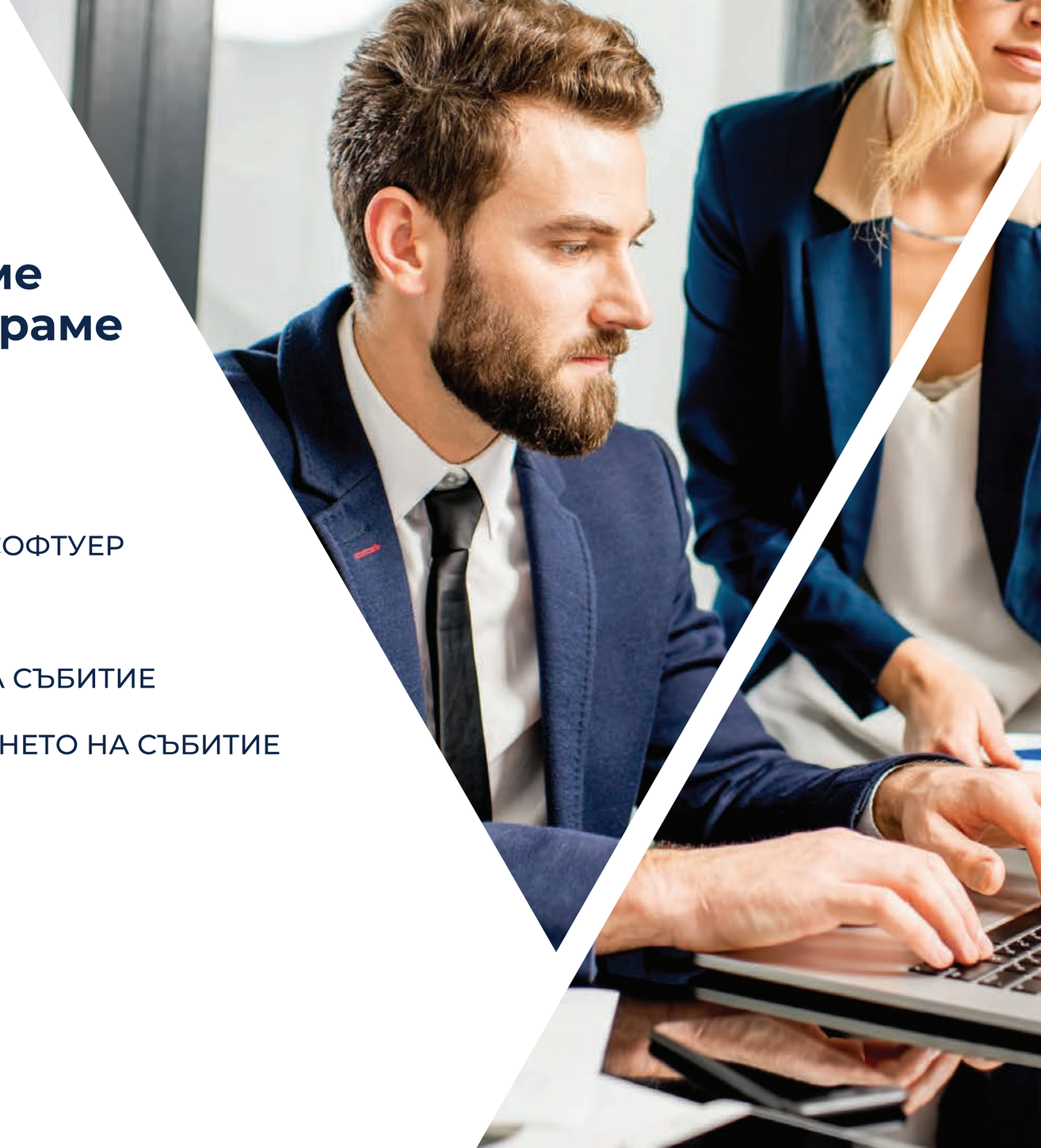
Cyber 360 ACADEMY

CYBER ONE

Вашето спокойствие е наш най-висок приоритет. Ние уважаваме вашата поверителност и ви гарантираме абсолютна конфиденциалност.

ПОКРИТИ РИСКОВЕ:

- ПРОБИВ В МРЕЖОВАТА СИГУРНОСТ ЧРЕЗ ЗЛОНАМЕРЕН СОФТУЕР
- КИБЕР ЗАПЛАХА ЗА ИЗНУДВАНЕ
- НЕОБХОДИМИ РАЗХОДИ СВЪРЗАНИ С НАСТЪПВАНЕТО НА СЪБИТИЕ
- ОТГОВОРНОСТ КЪМ ТРЕТИ ЛИЦА СВЪРЗАНА С НАСТЪПВАНЕТО НА СЪБИТИЕ
- МЕДИЙНА ОТГОВОРНОСТ
- 24/7 КИБЕРАСИСТАНС



ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

КАКВО ПОКРИВА КИБЕР ПОЛИЦАТА?

- Увреждане на цифрови активи
- Кибер прекъсване на дейността
- Кибер изнудване
- Реакция при пробив в информационната сигурност
- Кибертероризъм
- Лична репутация

ПОКРИТИЕ КЪМ ТРЕТИ СТРАНИ

- Претенции за отговорност относно поверителността
- Претенции за медийна отговорност
- Разходи, свързани със стандартите за сигурност на PCI DSS
- Регулаторна защита и санкции

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

Предотвратяване загубата на данни и информация следствие на хакерска атака

Предпазване на клиенти и партньори от въвличането им в мащабен кибер-инцидент

Грижа за сигурността на своите данни в случай на извънредна ситуация

Паричен ресурс за покриване на технически или правни разходи в случай на кибер-инцидент

ДОБРЕ ДОШЛИ ПРИ НАС!
ВИЕ НАПРАВИХТЕ ПЪРВАТА СТЪПКА КЪМ СВОЯТА ЗАЩИТА!

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ

БЛАГОДАРИМ ВИ!

ЗАСТРАХОВАТЕЛНА КОМПАНИЯ
ЛЕВ ИНС
АКТИВНАТА СИГУРНОСТ