ПРИМЕРИ НА ТИПИЧНИ ЗАКАНИ

Следната табела содржи примери на типични закани. Листата може да се користи при процесот на изработка на процената на ризик. Заканите може да бидат намерни, случајни или природни и може да резултираат со, на пример, оштетување или губење на основните функции. Следнава листа ги покажува заканите каде што Н е (намерно), С (случајно), П (природно). Н се користи за сите намерни дејства врз информатичките средства, С се користи за сите човекови активности што случајно може да ги оштетат информатичките средства и П се користи за сите инциденти што не се темелат врз човековите активности.

Тип	Закана	Потекло
Физички оштетувања	Пожар	С, Н, П
	Оштетување од вода	С, Н, П
	Загадување	С, Н, П
	Катастрофи	С, Н, П
	Уништување на опремата и медиумите	С, Н, П
	Прашина, корозија, замрзнување	С, Н, П
Природни настани	Климатски феномени	П
	Сеизмички феномени	П
	Метеоролошки феномени	П
	Поплави	П
Губење на основните услуги	Дефект на клима-уредите или снабдување на системот за вода	С, Н
	Дефект на доводот за струја	С, Н, П
	Дефект на телекомуникациската опрема	С, Н
Нарушување поради термичко зрачење	Електромагнетна радијација	С, Н, П
	Термална радијација	С, Н, П
	Електромагнетни пулсови	С, Н, П

Компромитирање на информациите	Пресретнување на компромитирачки сигнали	Н
	Далечинско шпионирање	Н
	Прислушување	Н
	Кражба на медиуми или документи	Н
	Кражба на опрема	Н
	Рециклирани или отфрлени медиумите	Н
	Обелоденување	С, Н
	Податоци од недоверливи извори	С, Н
	Упад во хардвер	Н
	Упад во софтвер	С, Н
	Откривање на локација	Н
Технички проблеми	Дефект на опремата	С
	Функционалност на опремата	С
	Презаситеност на информатичкиот систем	С, Н
	Функционалност на софтверот	С
	Одржување на информатичкиот систем	С, Н
Неовластени активности	Неовластено користење на опремата	Н
	Нелиценцирано копирање софтвер	Н
	Употреба на фалсификуван или копиран софтвер	С, Н
	Оштетување податоци	Н
	Незаконска обработка податоци	Н
Компромитирање на функциите	Грешки при работа	С
	Злоупотреба на права	С, Н
	Фалсификување права	Н
	Негирање постапки	Н
	Проблеми при достапност на персоналот	С, Н, П

Посебно внимание треба да се посвети на човековите закани. Тие се детаљно образложени во следната табела:

Потекло на закана	Мотивација	Можни последици
Хакери	Предизвик Его Побуна Статус Пари	• Хакирање • Социјален инженеринг • Упад во системот • Неовластен пристап во системот
Компјутерски криминал	Уништување информации Нелегално објавување информации Парична заработка Неовластено менување податоци	• Компјутерски криминал • Измамничко дело (на пример, лажно претставување и следење) • Информации за поткуп • Упад во систем
Терористи	Уцена Уништување Експлоатација Одмазда Политички придобивки Медиумска покриеност	• Бомби/тероризам • Информатичка војна • Напад врз системот • Пенетрација во системот • Упад во систем
Индустриска шпионажа (разузнавање, компании, странски влади, други владини интереси)	Конкурентна предност Економска шпионажа	• Одбранбена предност • Политичка предност • Економска експлоатација • Кражба на информации • Нарушување на приватноста • Социјален инженеринг • Навлегување во системите • Неовластен пристап до системите (пристап до класифицирани, лични

		информации поврзани со технологија).
Внатрешна закана (слабо обучени, незадоволни, злонамерни, несовесни, нечесни, или поранешни вработени)	Љубопитност Его Интелигенција Парична заработка Одмазда Ненамерни грешки и пропусти (на пример, грешка при внесување податоци, програмски грешки)	• Напад на вработен • Уцена • Пребарување на сопственички информации • Злоупотреба на компјутери • Измама и кражба • Поткуп за добивање информација • Внесување фалсификувани или компромитирани податоци • Следење • Продажба на лични податоци • Системски багови • Упад во системот • Саботажа на системот • Неовластени пристап во системот • Малициозен код (на пример: вирус, логичка бомба, тројански вирус)