

ПРЕГЛЕД НА РАНЛИВОСТИ

1. Примери за ранливост

Следната табела содржи примери на ранливости во различни области на безбедносната, вклучувајќи примери на закани што би можеле да ги искористат овие ранливости. Овие листи ќе помогнат во текот на изработката на процената на заканите и ранливостите со цел да се утврдат релевантни сценарија на инциденти. Треба да се потенцира дека во некои случаи некои други закани може да ги искористат истите овие ранливости.

| Типови | Примери на ранливости | Примери на закани |
|---------|---|--|
| Хардвер | Недоволно одржување / погрешна инсталација на медиуми за чување | Нарушување на одржувањето на информатичкиот систем |
| | Недостаток на периодични планови за замена | Уништување на опремата или на медиумите |
| | Подложност на влага, прашина, нечистотија | Прашина, корозија, замрзнување |
| | Чувствителност на електромагнетно зрачење | Електромагнетно зрачење |
| | Недостаток на ефикасна конфигурациска контрола | Грешка при употреба |
| | Подложност на напонски варијации | Губење на напојување |
| | Подложност на температурни варијации | Метеоролошки феномен |
| | Незаштитено складирање | Кражба на медиуми или документи |
| | Недостаток на грижа | Кражба на медиуми или документи |
| | Неконтролирано копирање | Кражба на медиуми или документи |
| Софтвер | Непостоење или недоволно тестирање софтвери | Злоупотреба на права |
| | Познати пропусти во софтверот | Злоупотреба на права |
| | Неодјавување при напуштање на работната станица | Злоупотреба на права |

| | | |
|-------|--|-----------------------------------|
| | Отстранување или повторна употреба на медиуми за чување, без соодветно бришење | Злоупотреба на права |
| | Недостаток на контролни траги | Злоупотреба на права |
| | Погрешна распределба на правата за пристап | Злоупотреба на права |
| | Широко дистрибуиран софтвер | Злоупотреба на податоци |
| | Примена на програми со погрешни податоци | Злоупотреба на податоци |
| | Комплициран кориснички интерфејс | Грешка во употреба |
| | Недостаток на документирање | Грешка во употреба |
| | Неправилно поставени параметри | Грешка во употреба |
| | Неточни датуми | Грешка во употреба |
| | Недостаток на механизми за идентификација и авторизација на корисникот | Фалсификување права |
| | Незаштитени табели со лозинки | Фалсификување права |
| | Лош менаџмент со лозинки | Фалсификување права |
| | Овозможени функции што не се неопходни | Незаконска обработка на податоци |
| | Нетестиран или нов софтвер | Нефункционирање на софтверот |
| | Нејасни или непотполни насоки дадени на програмерите | Нефункционирање на софтверот |
| | Недостатокот на ефективна контрола на промени | Нефункционирање на софтверот |
| | Неконтролирано симнување и употреба на софтвер | Упад во софтверот |
| | Недостаток на резервни копии | Упад во софтверот |
| | Недостаток на физичка заштита на објектот | Кражба на медиумите или документи |
| | Неуспех да се изготват извештаи за менаџирање | Неовластеното користење на опрема |
| Мрежа | Непостоење доказ за испраќање или примање порака | Негирање акции |
| | Незаштитени комуникациски линии | Прислушување |

| | | |
|---------------------|---|--------------------------------------|
| | Незаштитен сензитивен мрежен сообраќај | Прислушување |
| | Неквалитетен спој на каблите | Дефекти на телекомуникациска опрема |
| | Единечна точка на грешка | Дефекти на телекомуникациска опрема |
| | Недостиг на идентификација и авторизација на испраќачот и примачот | Фалсификување на правата |
| | Небезбедна мрежна архитектура | Шпионирање од далечина |
| | Пренос на лозинки во некриптирана форма | Шпионирање од далечина |
| | Несоодветното управување со мрежата | Заситеност на информатичкиот систем |
| | Незаштитени јавни мрежни конекции | Неовластено користење на опремата |
| Персонал | Отсуство на персоналот | Недостапност на персонал |
| | Несоодветни постапки при регрутација | Оштетување на опрема или медиуми |
| | Недоволна безбедносна обука | Грешка во употреба |
| | Неправилна употреба на софтвер и хардвер | Грешка во употреба |
| | Недостатокот на безбедносна свест | Грешка во употреба |
| | Недостаток на механизми за контрола | Незаконска обработка на податоци |
| | Непостоење надзор над работата на надворешните соработници и персоналот кој чисти | Кражба на медиумите или документи |
| | Недостаток на политики за правилна употреба на телекомуникациските пораки и медиуми | Неовластено користење на опремата |
| Местоположба | Несоодветно или негрижливо користење на контролите за физички пристап до објектите и просторите | Уништување на опремата или медиумите |
| | Локација во област подложна на поплави | Поплави |

| | | |
|--------------|---|--|
| | Нестабилна електричната мрежа | Губење на напојување |
| | Недостаток на физичка заштита на објектот, врати и прозорци | Кражба на опрема |
| Организација | Недостаток на формална процедура за регистрација и одјавување на корисникот | Злоупотреба на права |
| | Недостаток на формален процес за правото на преглед на пристап (контрола) | Злоупотреба на права |
| | Недостаток или недоволни одредби (во врска со безбедноста) во договорите со клиентите и / или со трети лица | Злоупотреба на права |
| | Недостаток на процедури за контролирање на објектите каде што се обработуваат информациите | Злоупотреба на права |
| | Недостаток на редовни контроли | Злоупотреба на права |
| | Недостаток на процедури за идентификација и процена | Злоупотреба на права |
| | Недостаток на извештаи за грешки евидентирани во административните и во оперативните логови | Злоупотреба на права |
| | Несоодветно реагирање при процесот на одржување | Нарушување на одржувањето на информатичкиот систем |
| | Недостаток или недоволно ниво на договорна услуга | Нарушување на одржувањето на информатичкиот систем |
| | Недостаток на процедурите за контрола на промени | Нарушување на одржувањето на информатичкиот систем |
| | Недостаток на формална процедура за документациска контрола | Злоупотреба на податоци |

| | |
|---|----------------------------------|
| Недостаток на формална процедура за контрола на евиденција | Злоупотреба на податоци |
| Недостаток на формални процеси за одобрување на јавно достапни информации | Податоци од недоворливи извори |
| Недостаток на правилна распределба на надлежностите во врска информатичката безбедност | Негирање на активности |
| Недостаток на план на континуитет | Дефект на опремата |
| Недостаток на политика за користење на e-mail | Грешка во употреба |
| Недостаток на процедури за воведување нов софтвер во оперативните системи | Грешка во употреба |
| Недостаток на записи во административните и оперативните логови | Грешка во употреба |
| Недостаток на процедури за ракување со класифицирани информации | Грешка во употреба |
| Недостаток на одговорности за информатичка безбедност во описот на работното место | Грешка во употреба |
| Недостаток или недоволно одредби (во врска со безбедноста на информациите) во договорите со вработени | Илегално процесирање на податоци |
| Недостаток на дефинирани дисциплински процеси во случај на безбедносен инцидент | Кражба на опрема |
| Недостаток на формална политика за користење лаптопи | Кражба на опрема |
| Недостаток на контрола на средствата коишто се за надворешна употреба | Кражба на опрема |

| | | |
|--|---|---|
| | Недостаток или недоволна политика на чиста маса и чист екран | Кражба на медиуми или документи |
| | Недостаток на овластување за објекти каде што се обработуваат информации | Кражба на медиуми или документи |
| | Недостаток на воспоставени механизми за мониторинг на безбедносни нарушувања | Кражба на медиуми или документи |
| | Недостаток на редовни прегледи од страна на менаџментот | Неовластено користење на опремата |
| | Недостаток на процедури за пријавување безбедносни слабости | Неовластено користење на опрема |
| | Недостаток на процедури и одредби во согласност со правата на интелектуалната сопственост | Употреба на фалсификувани или копирани софтвери |