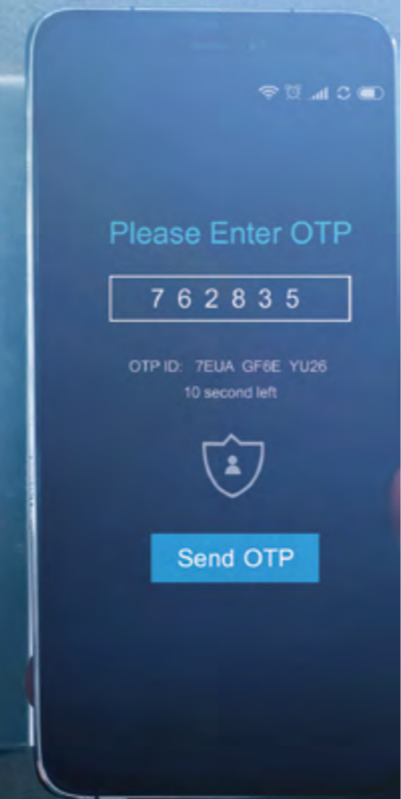


# РЕШЕНИЯ ЗА КИБЕРСИГУРНОСТ



# ЗАЩО КИБЕРСИГУРНОСТТА ИМА ЗНАЧЕНИЕ?

## CYBER SECURITY



Всеки ден ставаме все по зависими от киберпространството, глобалната дигитална инфраструктура за комуникации и информационен трансфер. Използваме ежедневно уеб-базирани услуги.

Потенциалните злонамерени атаки и заплахи могат да нанесат огромни вреди. Икономическите щети от киберпрестъпността са масивни и количествено измерими.

LIREX предлага широка гама решения за киберсигурност - системи за сигурност, които откриват и блокират съвременни и сложни атаки; средства за откриване и блокиране на потенциални изтичания на данни; възможност за интеграция и управление на мобилни устройства в корпоративни ИТ инфраструктури.

## НАШИТЕ РЕШЕНИЯ

ПОЛЗВАЙТЕ ГИ ВЕЧЕ С ВЪЗМОЖНОСТ ЗА МЕСЕЧЕН АБОНАМЕНТ

### NEXT-GENERATION FIREWALL

Блокирайте  
съвременните  
и сложни атаки

### EMAIL AND WEB SECURITY

Повишете сигурността на  
електронната пощенска  
и интернет услуга

### DATA LOSS PREVENTION

Предотвратете  
загубите на данни

### ENTERPRISE MOBILITY MANAGEMENT

Интегрирайте и защитете  
мобилните устройства  
в корпоративни ИТ  
инфраструктури

### END-POINT PROTECTION

Осигурете защита на  
настолни и мобилни  
устройства

### APPLICATION CONTROL/ LOAD BALANCER

Осигурете  
отказоустойчивост и  
повишена производителност

## NEXT-GENERATION FIREWALL

### БЛОКИРАЙТЕ СЪВРЕМЕННИТЕ И СЛОЖНИ АТАКИ

NGFW е решение за сигурност, което открива и блокира съвременни и сложни атаки.

Технологията интегрира три ключови характеристики за по-висока сигурност:

- Firewall функционалности
- Система за предотвратяване на проникване (intrusion prevention system - IPS)
- Контрол над приложенията (application control), носейки допълнителни функционалности при защита на важната за организацията информация.

NGFW спира атаки, базирани на изкуствен интелект /AI/ и дори ползва AI, за да блокира злонамерени действия.

Използваме NGFW решения на световните вендори Cisco, CheckPoint, PaloAlto, F5, Sophos.

## APPLICATION CONTROL /LOAD BALANCER/

### ОСИГУРЕТЕ ОТКАЗОУСТОЙЧИВОСТ И ПОВИШЕНА ПРОИЗВОДИТЕЛНОСТ

Съвременните информационни услуги трябва да бъдат достъпни по всяко време и да могат да поемат повишено натоварване, за да обслужват всички потребители, които се нуждаят от тях. За осигуряване на тези възможности използваме системи за отказоустойчивост и балансиране на натоварването. Тези системи осигуряват наличността, сигурността, видимостта на приложенията, както и ускорява тяхната работата. Процесът на балансиране на натоварването представлява разпределянето на данните върху няколко различни системи с цел осигуряване на отказоустойчивост, надеждност и повишена производителност.

Предлагаме ви решения на най-добрите на пазара - F5, Citrix, KEMP.

## E-MAIL & WEB SECURITY

### ПОВИШЕТЕ СИГУРНОСТТА НА ЕЛЕКТРОННАТА ПОЩЕНСКА И ИНТЕРНЕТ УСЛУГА

- Предотвратете загубата на данни, намалете риска от получавани съобщения от зловреден характер
- Намалете загубата на продуктивността и времето, което хората прекарват в интернет сърфиране
- Увеличете ефективността на персонала с намаляването на ненужните съобщения и фокусирането върху бизнес информацията и данни
- Повишете сигурността на web трафика – вероятността в даден website или web да бъде поместен зловреден код става все по-голяма, а от там и шансът крайно устройство във вашата организация да бъде заразено

Ключовите функционалности включват входящ и изходящ antispam, anti-malware, anti-virus, URL filtering, IP reputation, https криптиране.

Предлагаме решения на Cisco, Checkpoint, Symantec, Sophos, McAfee, Palo Alto.

## DATA LOSS PREVENTION (DLP)

### ПРЕДОТВРАТЕТЕ ЗАГУБИТЕ НА ДАННИ

Data Loss Prevention (DLP) решенията позволяват да се засичат потенциални проблеми чрез анализ на трафика и чувствителната информация, ценна за организацията и да се предотврати изтичането на поверителни данни. Ние ви предлагаме адекватни решения от водещи производители в областта. Това ще ви осигури:

- Единен интерфейс на управление
- Мониторинг на състоянието в реално време
- Възможности за дефиниране на собствени политики според нуждите
- Комплексна защита на данните
- Проактивност в борбата срещу загубата на информация

Предлагаме решения на Symantec, McAfee, Sophos, Microsoft 0365.

## END-POINT PROTECTION

### ОСИГУРИТЕ ЗАЩИТА НА НАСТОЛНИ И МОБИЛНИ УСТРОЙСТВА

Съвременният антивирусен софтуер вече не е само една програма за защита, а задължителен софтуерен компонент, важен инструмент за предотвратяване кражбата и загубата на данни и осигуряване на безопасна работа, както за бизнес клиенти, така и за крайни потребители.

Основните функции на антивирусните програми включват защита от:

- Threat Intelligence
- Sandboxing
- Point-in-Time откриване и блокиране на злонамерен софтуер
- Непрекъснат анализ, ретроспективна сигурност, корективни действия

Ние можем да ви помогнем както с консултация и анализ на вашите нужди, така и с проектиране и внедряване на антивирусни решения. Това ще ви осигури спокойствие и защитата на данните ви чрез блокиране на всякакви подозрителни или нежелани програми, безопасна работа при електронни разплащания и защита на мобилни устройства (телефони и таблети).

Предлагаме решения на Symantec, Sophos, McAfee, Cisco, Microsoft.

## FULL DISK ENCRYPTION

Цялостното криптиране на диска автоматично преобразува данните на твърдия диск във форма, която не може да бъде прочетена от друг. Без правилния ключ за удостоверяване, дори ако твърдият диск е свален и поставен в друга машина, данните остават недостъпни. Това е решение, подходящо за лаптопи и други малки устройства, които могат да бъдат физически загубени или откраднати. Решението е напълно в съответствие с изискванията на новия регламент GDPR за защита и криптиране на личните данни.

## ENTERPRISE MOBILITY MANAGEMENT (EMM) ТЕХНОЛОГИИ

### ИНТЕГРИРАЙТЕ И ЗАЩИТЕТЕ МОБИЛНИТЕ УСТРОЙСТВА В КОРПОРАТИВНИ ИТ ИНФРАСТРУКТУРИ

EMM инструментариумът конфигурира устройствата и приложенията за корпоративно внедряване, използване и управление на обновленията, спомага и за подмяна или премахване на устройствата от достъп до организацията.

EMM технологиите могат да проследяват и инвентаризират устройствата, настройките и използването им, за да се провери дали съответстват на корпоративните политики и дали управляват средствата за достъп.

EMM спомагат за предотвратяване на загубите на данни, кражби, или други инциденти чрез добавяне на контрол за шифриране на данните, права за достъп до данни, споделени устройства, приложение за опаковане и контейнери, както и "заклучване" на устройството.

ИТ отделът вече може и да проследява проблеми ситуации на мобилни устройства с достъп до мрежата чрез средствата на инвентаризация, анализ и отдалечено управление.

Предлагаме решения на VM ware Symantec, Checkpoint, Microsoft, Sophos.

НАД **10,000** КИБЕРАТАКИ  
НА ВСЕКИ ЧАС СЕ СЛУЧВАТ В СВЕТОВЕН МАЩАБ  
СТОЙНОСТТА НА ИКОНОМИКАТА НА КИБЕРПРЕСТЪПНОСТТА Е  
НАД **1 000 000 000 USD** ГОДИШНО\*

\*Данни на Институт за Киберсигурност

ЗАЩИТЕТЕ СВОИТЕ СИСТЕМИ  
с **LIREX**



НИЕ ВИ ОСИГУРЯВАМЕ ВСИЧКО ТОВА И ОЩЕ:



ОДИТ НА  
ТЕКУЩО СЪСТОЯНИЕ



ВНЕДРЯВАНЕ



ОПТИМИЗАЦИЯ НА  
ВНЕДРЕНИ РЕШЕНИЯ



ПРОЕКТИРАНЕ, ДИЗАЙН И  
ОСТОЙНОСТЯВАНЕ НА РЕШЕНИЯ  
ЗА ИНФОРМАЦИОННА СИГУРНОСТ



РАЗРАБОТВАНЕ  
НА ПРОЦЕДУРИ И  
ИНСТРУКЦИИ ЗА РАБОТА




ВАЛИДИРАНЕ НА КОНЦЕПЦИЯ  
"PROOF OF CONCEPT"



ПОДДРЪЖКА

# НАЙ-ДОБРИЯТ НАЧИН ЗА ЗАЩИТА ОТ ИЗТИЧАНЕ НА ДАННИ И ЧУВСТВИТЕЛНА ИНФОРМАЦИЯ Е ЕФЕКТИВНОТО РЕШЕНИЕ ЗА КИБЕРСИГУРНОСТ

 +359 2 9 691 691

 office@lirex.bg

 [www.lirex.bg](http://www.lirex.bg)

 Mladost 3, bl.306, Sofia 1712, Bulgaria

 LirexCom

 Lirex COM