DataLocker
Simply Secure

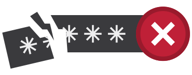
15 WAYS TO PREVENT THE BIGGEST DATA BREACH THREATS

Data breach is a bigger problem than ever and affects every industry. Luckily, there are a lot of basic things you can do to reduce your risk.

GLOBAL DATA BREACH

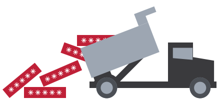
PROBLEM

80%



80% - Number of breaches from hacking involve brute force-attacks or the use of lost or stolen credentials.

40%



40% - Malware breaches that were the result of a password dumper.

SOLUTION

01

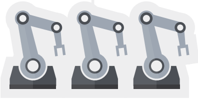
Implement/require stronger password policies

02

Use anti-malware tools on all end-points, including USB devices

03

Configure all USB storage devices to operate in Read-Only mode, especially if outside a trusted network.



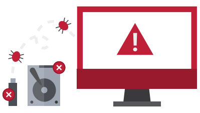
MANUFACTURING

PROBLEM

30%

30% - Manufacturing breaches with confirmed data loss were motivated by crimeware.

30%



30% - Manufacturing data breaches that were the result of malware (where malware made its way into endpoints and/or core infrastructure).

SOLUTION

04

Keep OT networks properly secure using air-gapped white-stationing protocols

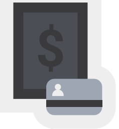
05

Use location-aware policy-controlled and fully-encrypted USB devices with onboard anti-malware to prevent whitestation intrusion.

06

Institute policy-based automations that define what file types can and cannot be stored on whitestation or OT-destined USB devices.

FINANCE



PROBLEM

28%

28% - Finance industry data breaches that came from "miscellaneous errors" such as errors making sure data storage was properly configured.

38%

38% - Finance industry data breaches that were the result of hacking (stolen credentials or backdoor exploits)

SOLUTION

07

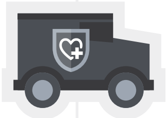
Institute policy-based automation that gives the workforce the security and flexibility they need without asking them to be security experts.

08

Roll-out endpoint management that ensures only approved USB storage devices can be used on any company-issued device.

09

Deploy routine audits of USB devices to ensure they are not being mis-used or exhibiting patterns of abuse or other data security threat.



HEALTHCARE

PROBLEM

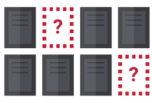
31%

31% - Healthcare industry data breaches that came from "miscellaneous errors" such as errors making sure data storage was properly configured.

32%

32% - Healthcare data breaches that were the result of simple errors such as not following established processes.

32%



32% - Healthcare data breaches that involved lost or stolen media.

SOLUTION

10

Use smart devices that can change their security posture automatically based on their location and the files being stored on them

11

Ensure these devices are secured with military-grade encryption trackable with routine audit reports.

12

Disable, erase, sanitize or remote detonate these devices if they are suspected of being lost or stolen

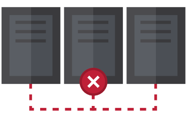
PUBLIC ADMIN / FED GOV

PROBLEM

63%

63% - Public administration security incidents motivated by crimeware.

32%



32% - Public administration industry data breaches resulting from "miscellaneous errors" such as errors making sure data

31%

31% - Public administration data breaches from hacking.

storage was properly configured.

SOLUTION

13

Manage one or thousands of people by groups, assigning security policies based on their role and access needs.

14

Deploy user-requestable trusted zones to certificate machines that should be safe to use.

15

Auto scan all new files added to USB storage devices for malware and either quarantine or destroy infected files.[1]

---

[1] Source: Verizon Data Breach Investigation Report 2020

HOW THE DL4 FE HELPS

A-Z
DATALOCKER

Many of the problems listed above involve bad processes and poor passwords. On some level, these are user-related issues. Using the DL4 FE, users can easily encrypt data on a powerful USB mass storage device. Meanwhile, admins can enforce automated policies that protect data, even in the face of malware or the occasional user error.

ON-BOARD DEVICE PROTECTION

DL4 FE can be set to read-only mode so that malware can't be written to the device. It can also be configured to disallow autoruns, so malware can't install itself. Plus, the DL4 FE can be set up with antimalware to quarantine/ delete malware that finds its way onto a device.

BRUTE FORCE PROTECTION

Brute force password protection ensures hackers can't simply defeat the device with brute force tactics. Complex passwords and a randomized keypad also prevent observers from copying passwords.

REMOTE DETONATE AND MANAGEMENT

The DL4 FE can be remotely locked, sanitized, or set to remote detonate (don't worry, it doesn't blow up, but all data and functionality does) protecting sensitive data. Admins can also remotely reset passwords if needed.

DATALOCKER®
SIMPLY SECURE

Get a Custom Demo

datalocker.com | sales@datalocker.com