

DATENSICHERUNG ALS LEBENSRETTETTER

Niklas Zistler

DIGITALE SICHERHEIT
ANPACKEN

#umsetzungstag



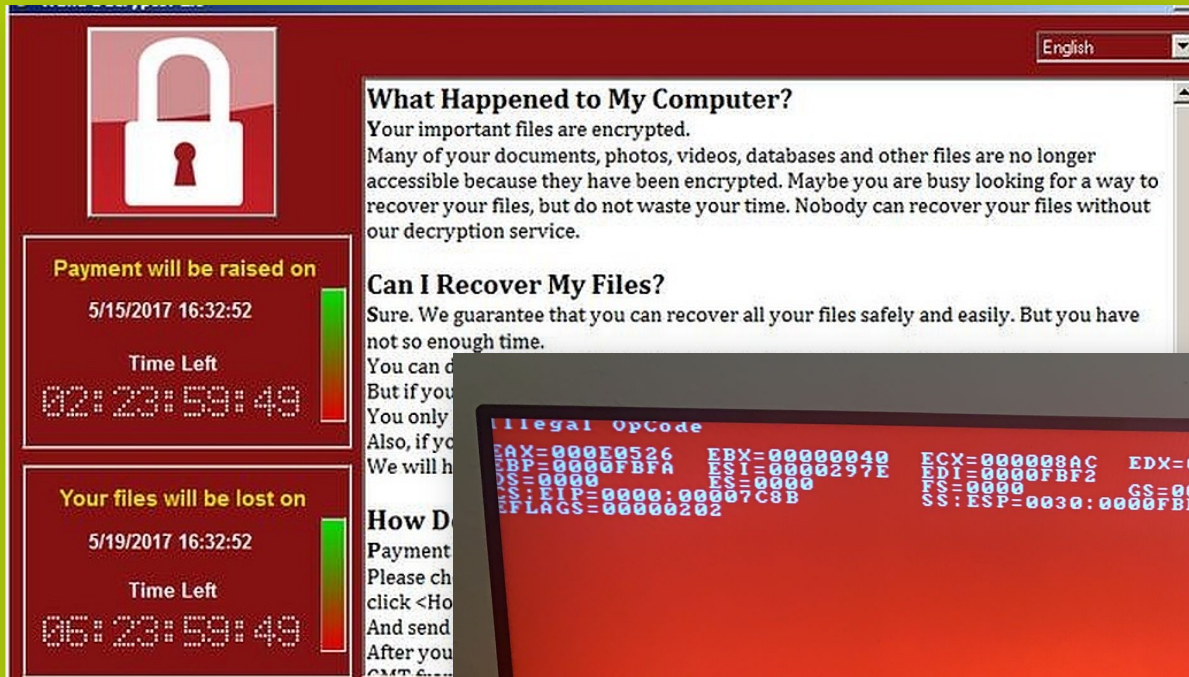
MEHRWERT EINER DATENSICHERUNG

- Datensicherung als „Lebensretter“
- schnell wieder handlungsfähig
- Schaden eines IT-Vorfalles minimieren

Erst gegeben, wenn ein passendes Konzept vorhanden ist!



AUS DER PRAXIS - RANSOMWARE



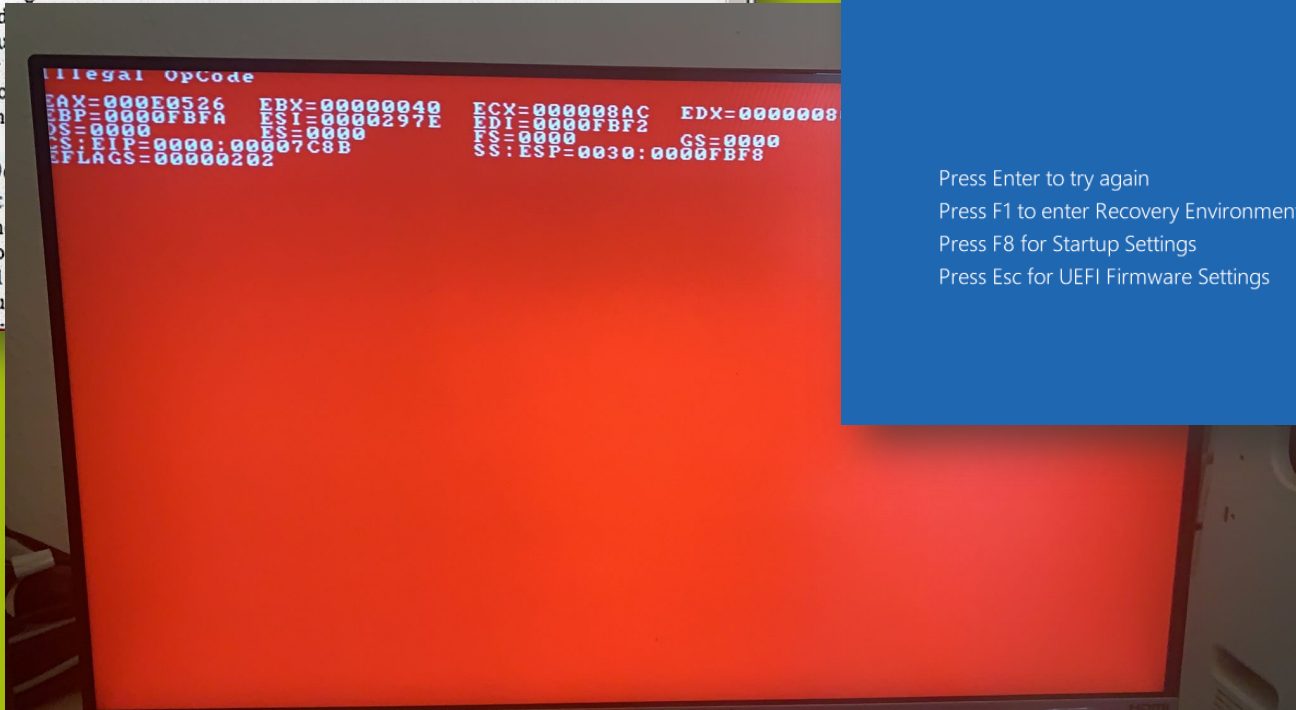
What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can do it. But if you don't. You only have 24 hours. Also, if you don't pay. We will delete your files.

How Do I Pay?
Payment must be made in Bitcoin. Please check the Bitcoin address and click <Home> to see the Bitcoin address. And send the Bitcoin to the address. After you send the Bitcoin, we will send you the decryption key.

Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49

Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49



Recovery

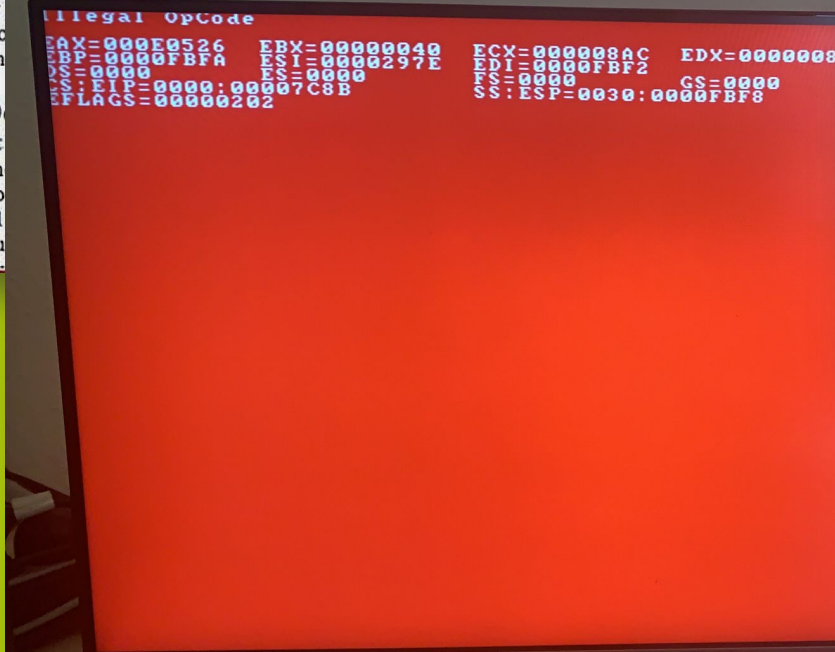
Your PC/Device needs to be repaired

A required device isn't connected or can't be accessed.

Error code: 0xc0000225

You'll need to use recovery tools. If you don't have any installation media (like a disc or USB device), contact your PC administrator or PC/Device manufacturer.

Press Enter to try again
Press F1 to enter Recovery Environment
Press F8 for Startup Settings
Press Esc for UEFI Firmware Settings



Illegal OpCode

```
AX=00000052 EBX=00000040 EBP=00000000 ESI=00000000 EDI=00000000  
ECX=00000000 EDX=00000000 EIP=00000000 IOPIC=00000000  
EAX=00000000 EBX=00000000 EBP=00000000 ESI=00000000 EDI=00000000  
ECX=00000000 EDX=00000000 EIP=00000000 IOPIC=00000000  
EAX=00000000 EBX=00000000 EBP=00000000 ESI=00000000 EDI=00000000  
ECX=00000000 EDX=00000000 EIP=00000000 IOPIC=00000000
```

LÖSEGELD BEZAHLEN?

- Darf das Lösegeld bezahlt werden?
- Kann das Lösegeld bezahlt werden?
- Sind Sie bereit, das Lösegeld zu bezahlen?
- Können Sie darauf vertrauen, dass eine Entschlüsselung überhaupt möglich ist?

DATEN WIEDERHERSTELLEN?

- Wann war die letzte Datensicherung?
- Waren die letzten Datensicherungen erfolgreich?
- Sind alle Systeme in der Datensicherung vorhanden?

HÄUFIGE FEHLER IM UMGANG MIT DATENSICHERUNGEN

Im schlimmsten Fall ist die Datensicherung nicht brauchbar!

- keine aktiven Kontrollen
- Datensicherungsmedium bleibt ständig angeschlossen
- Datensicherungen werden unverschlüsselt erstellt
- Wiederherstellbarkeit wird nicht getestet

Im schlimmsten Fall existieren keine Datensicherungen!

**WAS KÖNNEN SIE
ALSO TUN, UM
„SICHER“
AUFGESTELLT ZU
SEIN?**



3-2-1-PRINZIP

- 3 – Kopien der Daten
- 2 – Sicherungsmedien
- 1 – standortferne Kopie

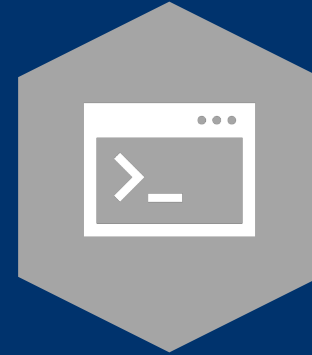
RESSOURCEN



Sicherungsplan



Sicherungsziel



Sicherungssoftware

Datensicherungskonzept

GRUNDLAGEN

Datensicherungen
anlegen

tägliche Kontrolle
der
Datensicherung

Datensicherung
vom System
trennen

Wiederherstell-
barkeit testen

EMPFEHLUNGEN

- bei Veränderung: Datensicherung auf Vollständigkeit und Funktion überprüfen
- Wiederherstellung nach Schadware: Virenprüfung der Systeme nach/während der Wiederherstellung
- System sollten nach einer Kompromittierung neu erstellt werden

GRENZEN VON INTEGRIERTEN LÖSUNGEN

Windows Server Sicherung

- kostenlos und im Betriebssystem integriert
- verhältnismäßig einfach zu bedienen

Kostenpflichtige Software

- Verschlüsselung der Datensicherung
- mehrstufige Datensicherung

AN DIE SICHERUNG DER CLOUD GEDACHT?

- unabhängige Wiederherstellung
- Datensicherung unter eigener Kontrolle
- Cloud Exit-Strategie



SICHERUNG DER CLOUD

In NAS-Systemen integrierte Lösungen

- häufig Lizenzkostenfrei
- NAS-System häufig bereits vorhanden

Softwarelösungen

- weiteres Gerät wird benötigt
- häufig kostenlos für eine bestimmte Anzahl an Nutzern

LEARNINGS

- Datensicherungen anlegen
 - verschlüsselt
 - offline Datensicherungen trennen
- tägliche Kontrolle der Datensicherung
- Wiederherstellbarkeit testen



CHEAT SHEET

Ressourcen

- Sicherungsplan
- Sicherungsmedium
- 3-2-1-Prinzip
- Sicherungssoftware

Datensicherungen

- verschlüsselt anlegen
- tägliche Kontrollen
- Sicherungsmedium trennen

Cloud

- Cloud-Daten sichern
- lokale Sicherung vorhanden

Empfehlung

- 1x pro Jahr die Wiederherstellbarkeit testen lassen
- Datenwiederherstellung mit Virenprüfung

Kompetenzzentrum für Cybersicherheit in der Wirtschaft in NRW

Die Grundlagen der Digitalen Sicherheit sind nicht aufwändig in der Umsetzung, aber wirkungsvoll für den Schutz Ihrer Digitalen Daten und Wertgegenstände.

Besuchen Sie unsere Website: www.digital-sicher.nrw

Adresse

Standort Bochum
Lise-Meitner-Allee 4
44801 Bochum

Standort Bonn
Rheinwerkallee 6
53227 Bonn

Kontakt

 +49 234 - 5200 7334

 info@digital-sicher.nrw

Social Media



**DIGITAL
SICHER
NRW**