

Sunteți pregătiți pentru aplicarea GDPR?

Știți unde se află Datele cu Caracter Personal din organizația / compania dumneavoastră ca să le puteți proteja?

Cum ar fi să vă protejați datele cu caracter personal folosind un algoritm de criptare recomandat de NSA (National Security Agency din SUA) și clasificat ca Suite B Cryptography¹?

ScanZitive și kryptOn – două utilitare *pentru fiecare zi* în protecția datelor personale

25 mai 2018 este data intrării în vigoare a REGULAMENTULUI (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal (Regulamentul general privind protecția datelor). Regulamentul are o serie de prevederi obligatorii pentru statele membre, pentru care nu mai este necesară preluarea în legislația națională pentru a fi aplicate (ca în cazul Directivelor). Penalitățile prevăzute sunt extrem de severe (merg până la 4% din cifra globală de afaceri a unui grup de companii sau 20 milioane de EURO, care dintre cele două **este mai mare**).

Un studiu al International Data Corporation (IDC – principalul furnizor global de servicii de analiză de piață pentru domeniul IT&C) din 2014 arată că în medie, 20.8% din informațiile unei organizații sunt date "structurate", gestionate în aplicații specializate sau baze de date. În acest caz, protecția datelor se reduce la mecanismele interne prevăzute de dezvoltatorul aplicației. Protejarea lor trebuie gestionată pe baza relației cu acești furnizori.

Restul de **79,2% din informații sunt date "nestructurate", găzduite în fișiere** răspândite pe serverele și PC-urile organizației. Ritmul mediu anual de creștere pentru date (structurate și nestructurate) este de 42,5% ceea ce **obligă la existența unei preocupări permanente** pentru administrarea acestor informații. Protejarea Datelor cu Caracter Personal aflate în fișiere revine ca responsabilitate în mod direct organizației respective. ScanZitive este un software utilitar care vă permite să identificați prezența datelor cu caracter personal (dar și orice alte informații) în informația nestructurată.

Utilizarea este ultra-simplă în ambele cazuri și presupune 3 pași:

ScanZitive	kryptOn
1. Stabiliți secvențele de date senzitive pe care doriți să le căutați 2. Rulați utilitarul ScanZitive și aflați unde se află datele căutate 3. Decideți ce doriți să faceți cu informația senzitivă.	1. Stabiliți fișierele de date senzitive pe care doriți să le criptați 2. Rulați utilitarul kryptOn și criptați fișierele 3. Ori de câte ori aveți nevoie, decriptați cu kryptOn, prelucrați informația și repetați pasul 2.

¹ https://en.wikipedia.org/wiki/NSA_Suite_B_Cryptography

Se recomandă pașii de mai sus să fie realizați cu o periodicitate care depinde de rata înnoirii informației senzitive.

De ce ScanZitive? – conformitatea cu GDPR

Pentru a putea respecta drepturile persoanelor vizate și îndeplini obligațiile operatorului în relația cu acestea și a răspunde cu ușurință și corect cererilor privind exercitarea de către persoanele vizate a drepturilor lor **trebuie să existe un control clar asupra existenței și localizării DCP², inclusiv pentru cazul în care acestea rezidă în fișiere, ceea ce se poate realiza cu ScanZitive.** Pe scurt, aceste drepturi includ:

1. Dreptul de acces (bazat pe imagine clară și corectă cu privire la DCP colectate legal și stocate)
2. Dreptul la rectificare
3. Dreptul la ștergere (uitare)
4. Dreptul la restricționarea prelucrării
5. Obligația de notificare la rectificare, ștergere, restricționare
6. Dreptul la portabilitatea DCP
7. Dreptul la opoziție la prelucrarea DCP
8. Restricții pentru decizii automatizate ale Operatorului

În conformitate cu **Articolele 13, ...,23**

În conformitate cu **Articolul 28 - Persoana împuternicită de operator**

PIO trebuie, la alegerea operatorului, **să șteargă sau să returneze** toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, [...] ceea ce presupune și pentru PIO³ existența unui control clar asupra DCP existente, control realizabil cu **ScanZitive**.

În conformitate cu **Articolul 30 – Evidențele activităților de prelucrare**

Operatorul și PIO, păstrează **o evidență** a tuturor categoriilor de activități de prelucrare desfășurate.

De ce criptare, de ce kryptOn ?

Preambulul Regulamentului

„În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui

- *să evalueze riscurile inerente prelucrării și*
- *să implementeze măsuri pentru atenuarea acestor riscuri, cum ar fi criptarea.”*

Articolul 6 – Legalitatea prelucrării

Aliniatul (4):

" În cazul în care prelucrarea

în alt scop decât cel pentru care datele cu caracter personal au fost colectate

nu se bazează pe

- consimțământul persoanei vizate sau pe
- dreptul Uniunii sau
- dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la articolul 23 alineatul (1),

operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial,

² DCP – Date cu Caracter Personal

³ PIO – Persoana Împuternicită de Operator

ia în considerare, printre altele: [...]

(e) ***existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.***

Articolul 24 - Responsabilitatea operatorului

(2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alineatul (1) includ punerea în aplicare de către operator a unor ***politici adecvate de protecție a datelor***.

Articolul 32 – Securitatea prelucrării

Aliniatul (1)

Având în vedere

stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice,

operatorul și persoana împuternicită de acesta

implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz: [...]

(a) ***pseudonimizarea și criptarea*** datelor cu caracter personal;

Articolul 34 Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

(3) Informarea persoanei vizate menționată la alineatul (1) nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

(a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, ***cum ar fi criptarea***;

În rezumat, Regulamentul instituie 3 mari categorii de obligații pentru operatorii de DCP și Persoanele Împuternicite de Operatori:

1. Obligații legate de respectarea drepturilor persoanelor vizate în legătură cu prelucrarea datelor lor personale (de la colectare la distrugere)
2. Obligații legate de protecția DCP
3. Obligații referitoare la menținerea de evidențe cu privire la prelucrarea DCP

ScanZitive susține activitățile legate de punctele 1 și 3 pentru DCP stocate nestructurat, în fișiere; kryptOn asigură (pentru aceleași DCP protecția prin criptare).

Despre ScanZitive

ScanZitive caută secvențele de text definite de utilizator într-un fișier de tip .txt în cele mai uzuale categorii de fișiere dintr-un director specificat:

 .docx	 .xlsx	 .pptx
 .doc	 .xls	 .pdf
 .odt	 .ods	 .odp
 .ott	 .ots	 .otp
 .json	 .csv	 .txt
 .jpeg	 .png	 .tif

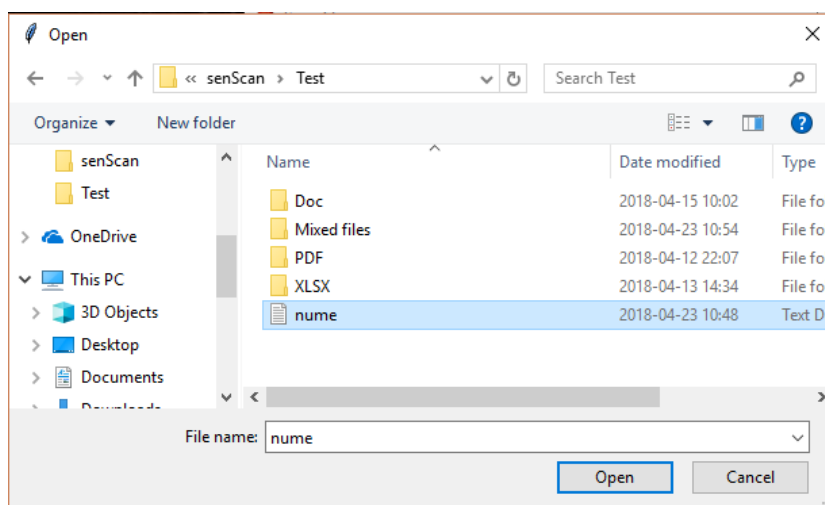
Utilitarul deschide pe rând toate fișierele din categoriile menționate și verifică prezența a cel puțin una dintre secvențele de text căutate.

Utilizarea este foarte simplă.

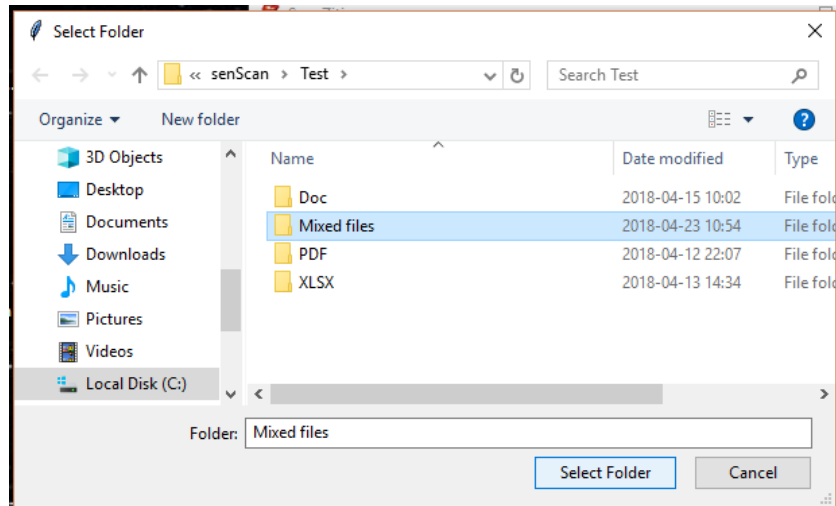
Dublu-click pe icon-ul aplicației:



Aplicația vă cere să selectați fișierul de secvențe de text (nume, prenume, CNP-uri, adrese de mail, numere de telefon, etc.) după care vreți să se facă căutarea (Fișierul de Intrare):



Apoi, trebuie să selectați directorul în care doriți să se facă căutarea (căutarea se va face automat în toate directoarele subordonate celui ales):

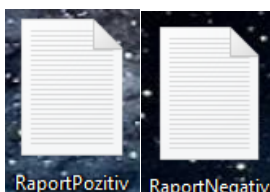
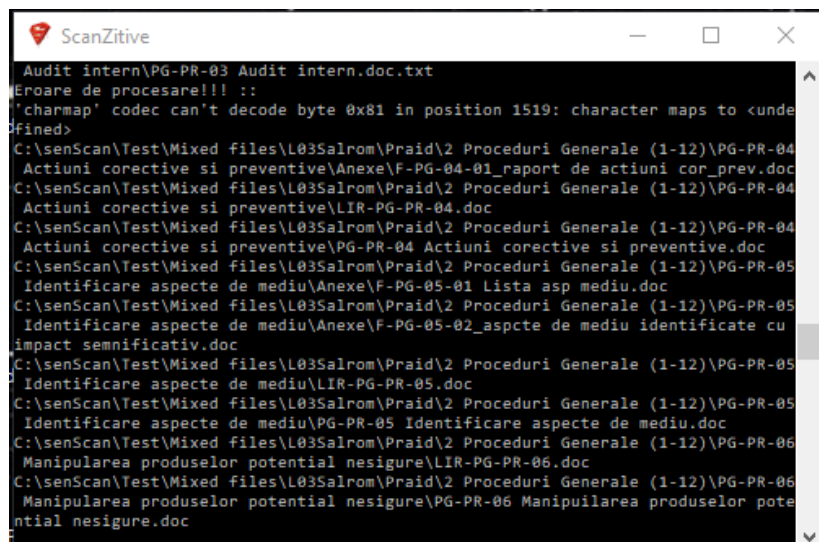


Aplicația demarează căutarea. Viteza depinde de numărul și volumul secvențelor de text căutate și de caracteristicile calculatorului pe care se face căutarea și se poate situa undeva între 1 și 4 GB pe oră. În paralel cu căutarea (care poate dura ore) puteți lucra la sarcinile dvs. curente.

Pe durata căutării, aplicația afișează pe rând fișierele scanate.

Toate fișierele pentru care rezultatul căutării a fost pozitiv sunt listate într-un fișier .txt numit "Raport pozitiv".

Toate fișierele de alt tip care nu au putut fi verificate și fișierele care au dat erori la verificare sunt listate într-un fișier .txt numit "Raport negativ".



La încheierea căutării, deschideți fișierul "RaportPozitiv" pentru a vedea calea, denumirile fișierelor și prima secvență găsită în fișierul respectiv. Pentru aceste fișiere, va trebui să decideți ce măsuri și ce nivel de protecție veți adopta în funcție de riscurile cu care vă confrunțați.

Similar, deschideți fișierul "RaportNegativ" pentru a vedea calea, denumirile fișierelor și cauza pentru care respectivele fișiere nu au putut fi scanate cu succes. Pentru aceste fișiere, va trebui să adoptați o altă cale de analiză privind prezența datelor cu caracter personal.

Limitări ale răspunderii

ScanZitive a fost dezvoltat pentru a realiza căutarea în mod specific pentru anumite formate de fișiere, enumerate mai sus. Chiar și în cazul acestor fișiere, există situații excepționale în care găsirea/detectarea unei anumite secvențe nu este posibilă. Între acestea enumerăm:

- secvența se găsește în interiorul unei imagini încorporate în fișierul analizat (de exemplu fotografia unui text inclusă într-un document MS Word);
- secvența se găsește în interiorul unor fișiere care nu respectă întocmai specificațiile aplicațiilor care le-au produs (MS Office, PDF, etc.) ,
- Secvența nu poate fi găsită din motive care depind de limitele tehnologiei de dezvoltare utilizate, a erorilor de funcționare ale sistemului de operare sau ale altor straturi software intermediare,
- alegerea secvențelor de utilizat în căutare este un aspect esențial pentru eficacitatea detectării informațiilor senzitive și revine beneficiarului, chiar dacă, odată cu aplicația, furnizorul pune la dispoziție și un Fișier de Intrare exemplificativ care poate fi utilizat în căutarea informației
- alegerea secvențelor de utilizat în căutare este un aspect esențial pentru eficiența detectării informațiilor senzitive și revine beneficiarului; căutarea este "case sensitive" ceea ce înseamnă că o secvență scrisă cu majuscule este distinctă de una scrisă cu minuscule; de asemenea, în cadrul Raportului Pozitiv pot fi incluse și fișiere "fals pozitive": dacă una dintre secvențele declarate de căutare este "Ana" (în Fișierul de Intrare), atunci aplicația va include în fișierul RaportPozitiv.txt și fișiere care conțin de exemplu fragmentul de text "**Analiza** factorilor este..." deoarece acest fragment include secvența de căutare respectivă.
- În cazul celor trei formate de fișiere de tip grafic/imagine (JPEG, PNG, TIFF), identificarea secvențelor de text depinde de o multitudine de factori: calitatea imaginii (zgomot scăzut), contrastul între text și fundal, etc. și este condiționată de stadiul actual, încă limitat, al funcționalităților de recunoaștere de caractere.

Utilitarul împarte fișierele analizate în trei mari categorii:

1. Fișiere în care a fost găsită cel puțin o secvență din secvențele enumerate în Fișierul de Intrare - fișierele sunt enumerate în fișierul "RaportPozitiv.txt" împreună cu calea asociată și prima secvență de căutare găsită în interiorul lor)
2. Fișiere care din diferite motive nu au putut fi analizate (fișiere corupte, formate de fișiere neprelucrate de utilitar) – aceste fișiere sunt enumerate în fișierul "RaportNegativ.txt" împreună cu calea asociată;
3. Fișiere care au putut fi analizate dar în care nu au fost găsite secvențe din Fișierul de Intrare.

În consecință, ScanZitive este un instrument util în detectarea și localizarea informației senzitive din organizații, fără a înlocui/elimina alte mijloace de administrare a informației senzitive și de analiză a riscurilor asociate și fără a garanta (așa cum s-a explicat mai sus) detecția exhaustivă a informației senzitive. Deciziile privind protecția informațiilor senzitive și punerea lor în aplicare revin integral beneficiarului. La modul general, răspunderea pentru maniera corectă de utilizare a aplicației revine beneficiarului.

Baza legală a furnizării aplicației informatice ScanZitive

Utilitarul ScanZitive se încadrează la Art. 31. Pct g) al ordonanței 25/2006 - Ordonanța nr. 25/2006 privind întărirea capacității administrative a Oficiului Român pentru Drepturile de Autor: "*programe pentru calculator destinate utilizării interne de către instituții, organizații sau operatori economici și actualizările acestor programe cu condiția de a nu fi distribuite prin magazine*"

Despre kryptOn

kryptOn criptează orice fel de fișier.

Operațiunile sunt următoarele:

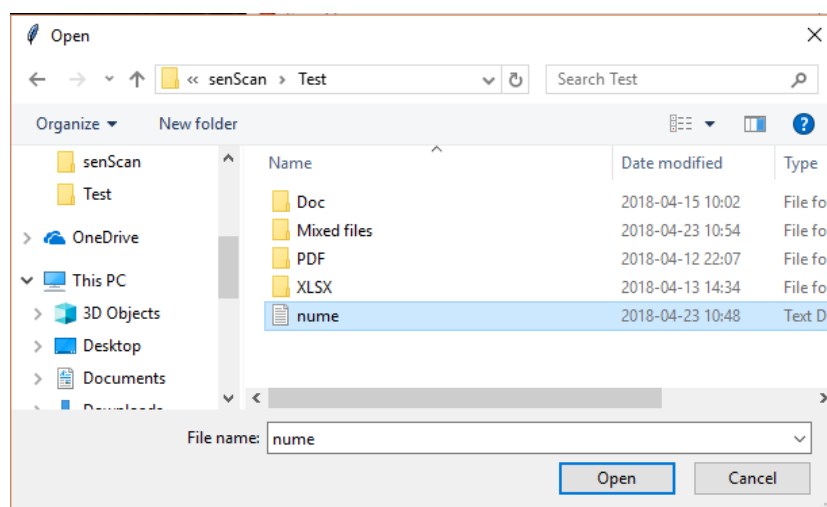
Dublu-click stânga pe icon-ul aplicației:



Aplicația vă cere să alegeți modul în care o veți utiliza. Aveți următoarele posibilități: criptare/decriptare individuală de fișiere, criptarea / decriptarea unui întreg director și a subdirectoarelor sale, criptarea unei liste de fișiere (așa cum este ea generată de utilitarul ScanZitive (RaportPozitiv sau RaportNegativ)).

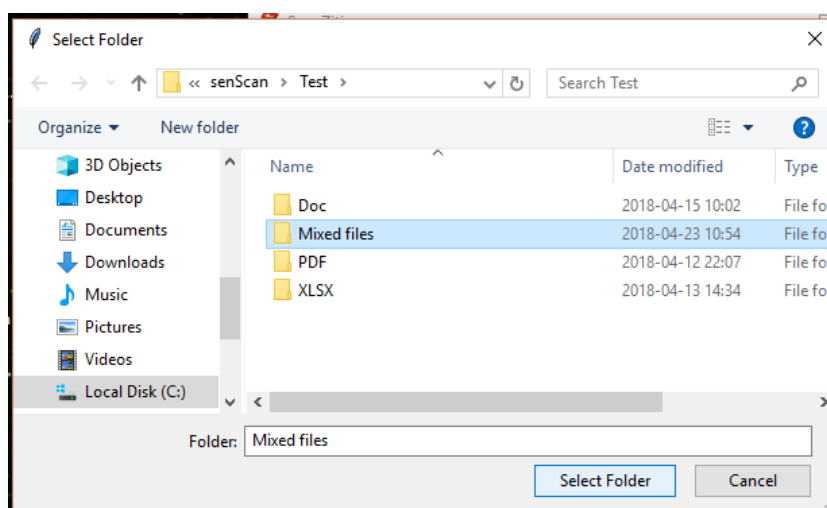


În cazul criptării/decriptării individuale de fișiere sau al criptării unei liste de fișiere, aplicația vă cere să selectați fișierul corespunzător (Fișierul de Intrare):



Lista de fișiere poate fi cea preluată de la rezultatul căutării cu ScanZitive sau poate fi editată manual cu orice editor de text (de exemplu NotePad).

În cazul în care doriți să criptați/decriptați un întreg director, aplicația vă cere să selectați directorul respectiv (criptarea se va face automat în toate directoarele subordonate celui ales):



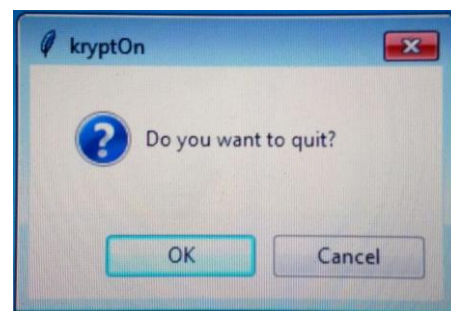
Aplicația demarează criptarea. Viteza depinde de numărul și volumul fișierelor de criptat și de caracteristicile calculatorului pe care se face criptarea. În paralel cu criptarea (care poate dura ore în cazul volumelor de ordinul zecilor de GB și secundelor-zecilor de secunde în cazul unui singur fișier) puteți lucra la sarcinile dvs. curente.

Odată încheiată criptarea, aplicația afișează în fereastra consolă (neagră) operațiile efectuate și puteți relua operația de criptare/decriptare pentru alte fișiere / directoare.

În cazul în care doriți să ieșiți din aplicație, dați click pe butonul  din colțul dreapta-sus al ferestrei.



Odată ce ați dat click, o a doua fereastră vă va întreba dacă doriți într-adevăr să ieșiți din aplicație.



Limitări ale răspunderii

kryptOn a fost dezvoltat utilizând unul dinre cei mai siguri algoritmi utilizați la ora actuală, recomandat și de National Security Agency și inclus în categoria "B" de algoritmi de criptare pentru autoritățile SUA, inclusiv pentru informații clasificate⁴.

Nu există vulnerabilități cunoscute pentru acest algoritm și nici pentru funcția de implementare curent utilizată pentru produsul **kryptOn**. Puteți citi mai multe [aici](#) și [aici](#). Pentru a cita o opinie de pe ultimul site referit: "dacă s-ar încerca decriptarea pe 1000 de miliarde de calculatoare, care fiecare ar putea testa un miliard de chei de criptare pe secundă, ar dura mai mult de 2 miliarde de ani pentru a sparge o criptare AES făcută cu o cheie de 128 de biți.". **kryptOn** folosește o cheie de 256 de biți.

Viteza de criptare este de regulă între 30-100+ GB pe oră, depinzând de caracteristicile calculatorului pe care rulează.

În consecință, **kryptOn** este un instrument util în protejarea informației sensitive din organizații, fără a înlocui/elimina alte mijloace de administrare a informației sensitive și de analiză a riscurilor asociate, fără a rezolva toate cerințele Regulamentului (UE) 2016/679 și fără a garanta (așa cum s-a explicat mai sus – nu există vulnerabilități **cunoscute**) protecția absolută a informației sensitive. Deciziile privind protecția

⁴ <https://www.nsa.gov/search/?q=AES+256>

informațiilor senzitive și punerea lor în aplicare revin integral beneficiarului. La modul general, răspunderea pentru maniera corectă de utilizare a aplicației revine beneficiarului.

Atenție !!!

Dacă alegeți să criptați din greșeală un director de pe hard disk care conține de exemplu fișiere de sistem, **e ca și cum ați șterge acel fișier din greșeală**: calculatorul dvs. va înceta să funcționeze corect sau va înceta să funcționeze pur și simplu, existând șansa să pierdeți toate datele. Deci, **separați clar datele senzitive și datele de business de aplicațiile informatice și fișierele de sistem** și utilizați cu atenție **kryptOn**.

Mutați fișierele cu date senzitive și de business, inclusiv de pe desktop într-un director de pe C: sau alt hard disk, de exemplu **C:\business\...** sau **D:\business\...** în afara directoarelor

C:\Program Files

C:\Program Files (x86)

C:\Users

C:\AppData

C:\ScanZitive

(în funcție de versiunea de sistem de operare și aplicațiile instalate, pot exista și alte directoare de sistem !)

Mulți utilizatori nu știu faptul că zona "Desktop" este într-un director sistem (de exemplu pentru utilizatorul cu username-ul "Adrian", calea este de fapt C:\Users\Adrian\Desktop). Prin urmare, nu țineți niciun fel de informații senzitive sau de business pe Desktop (sau într-un subdirector). Dacă ScanZitive găsește fișiere cu date senzitive pe Desktop sau subdirectoarele sale; vă recomandăm să le mutați în afara directoarelor de sistem și să mai rulați o dată **ScanZitive** pentru a vă asigura că n-ați omis nimic. Înainte de a rula **kryptOn** pe liste de fișiere sau directoare, asigurați-vă (rulând eventual de mai multe ori **ScanZitive**) că nu au mai rămas fișiere cu date personale în directoarele / subdirectoarele de sistem. Studiați cu mare atenție lista și căile fișierelor din RaportPozitiv și RaportNegativ generate de **ScanZitive** pentru a vă asigura că nu sunt incluse căi care conțin directoare/subdirectoare de sistem. În general, utilizați cu precauție criptarea pe liste de fișiere și directoare.

În cazul în care ați criptat din greșeală un director care nu trebuia criptat, nu închideți aplicația și efectuați imediat operația inversă.

În general evitați criptarea pe loturi de fișiere – de preferat să criptați fișier cu fișier.

Totodată, în momentul în care demarați criptarea, asigurați-vă că niciunul dintre documentele de criptat nu este deschis. Într-un asemenea caz, criptarea se va realiza fără a putea șterge fișierul sursă la final deoarece sistemul de operare nu permite acest lucru (fișierul fiind deschis și de o altă aplicație). În consecință veți avea atât fișierul în clar cât și cel criptat. De asemenea, dacă userul care rulează kryptOn nu are drepturi de scriere pe un fișier, operațiile encrypt/decrypt vor esua pe acel fișier. Se poate ca un user să aibă doar drept de citire pe un fișier, nu și drept de scriere!!

Furinzorul **nu își asumă nicio răspundere pentru utilizarea greșită a aplicației kryptOn**.

Baza legală a furnizării aplicației informatice

Utilitarul **kryptOn** se încadrează la Art. 31. Pct g) al ordonanței 25/2006 - Ordonanța nr. 25/2006 privind întărirea capacității administrative a Oficiului Român pentru Drepturile de Autor: "programe pentru calculator

destinate utilizării interne de către instituții, organizații sau operatori economici și actualizările acestor programe cu condiția de a nu fi distribuite prin magazine”

Licențe

Pentru ambele aplicații, licențele se acordă pentru stații de lucru / PC-uri cu Windows 7, 8, 10, pe o perioadă de 1 an.