

Introducere

Tehnologia informației specifică componentele care sunt utilizate pentru a stoca, prelua și manipula informațiile la nivelul minim, cu serverul care are un sistem de operare. Tehnologia informației are o gamă largă de aplicații în educație, afaceri, sănătate, industrii, sectorul bancar și cercetarea științifică la un nivel mare. Odată cu avansul principal în tehnologia informației, este necesar să aveți cunoștințe despre problemele de securitate, de confidențialitate și de principalele efecte negative ale IT. Pentru a face față acestor probleme în societatea IT este important să aflăm problemele etice.

Codul etic, în general, abordează modul în care principiile etice fundamentale sunt aplicate comportamentului unui profesionist IT. Codul nu este un algoritm pentru rezolvarea problemelor etice; mai degrabă, servește ca punct de plecare pentru luarea deciziilor etice. Când abordează o anumită problemă, un profesionist în informatică poate fi confruntat cu principii multiple care trebuie luate în considerare, iar aceste principii pot prezenta diferite grade de relevanță pentru problema abordată. La întrebările legate de aceste tipuri de întrebări se poate răspunde cel mai bine printr-o analiză atentă a principiilor etice fundamentale, cu binele public ca prioritate. Întreaga profesie IT beneficiază atunci când procesul de luare a deciziilor etice este responsabil și transparent față de toate părțile interesate. Discuțiile deschise pe probleme etice promovează responsabilitatea și transparența.

Unele dintre problemele etice majore cu care se confruntă tehnologia informației (IT) sunt:

1. Confidențialitate personală
2. Dreptul de acces
3. Acțiuni dăunătoare
4. Brevete

5. Drepturi de autor
6. Secretele comerciale
7. Răspunderea
8. Pirateria

Confidențialitate personală

Este un aspect important al problemelor etice în tehnologia informației. IT facilitează utilizatorilor să aibă propriul hardware, sistem de operare și instrumente software pentru a accesa serverele conectate între ele și la utilizatori printr-o rețea. Datorită distribuției rețelei la scară largă, are loc transferul de date sau informații într-o cantitate mare, ceea ce duce la șansele ascunse de a divulga informații și de a încălca confidențialitatea oricărei persoane sau a unui grup. Este o provocare majoră pentru societatea și organizațiile IT să păstreze confidențialitatea și integritatea datelor. Divulgarea accidentală către persoane necorespunzătoare și dispozițiile pentru a proteja acuratețea datelor apar, de asemenea, în problema confidențialității.

Profesioniștilor IT li se încredințează adesea informații confidențiale, cum ar fi secrete comerciale, date despre clienți, strategii de afaceri non-publice, informații financiare, date de cercetare, articole științifice nepublicate și cereri de brevet. Profesioniștii IT trebuie să protejeze confidențialitatea, cu excepția cazurilor în care găsesc dovezi ale încălcării unei legi, a reglementărilor organizației sau a Codului. În aceste cazuri, natura sau conținutul acestor informații trebuie comunicate numai autorităților corespunzătoare. Un profesionist în informatică ar trebui să evalueze cu atenție dacă astfel de dezvăluiri sunt conforme cu Codul.

Dreptul de acces

Dreptul de acces devine o problemă de înaltă prioritate pentru IT și spațiul cibernetic, cu un mare progres în tehnologie. Comerțul electronic și evoluția sistemelor de plăți electronice pe internet au sporit această problemă pentru diferite organizații corporative și agenții guvernamentale. Rețeaua de pe internet nu poate fi securizată de accesul neautorizat. În general, sistemul de detectare a intruziunilor este utilizat pentru a determina dacă utilizatorul este un intrus sau un utilizator adecvat.

Acțiuni dăunătoare

Acțiunile dăunătoare din etica IT se referă la daunele sau consecințele negative asupra IT, cum ar fi pierderea informațiilor importante, pierderea proprietății, pierderea proprietății, distrugerea proprietății și impacturi substanțiale nedorite. Acest principiu de conduită etică restricționează orice persoană din afară de la utilizarea tehnologiei informației într-o manieră care duce la orice pierdere pentru oricare dintre utilizatori, angajați, angajatori și publicul larg. De obicei, aceste acțiuni cuprind distrugerea sau modificarea intenționată a fișierelor și a programului, ceea ce determină o pierdere gravă de resurse. Pentru a recupera din acțiunile dăunătoare, sunt necesare eforturi suplimentare pentru a elimina virusii din sistemele informatice.

Brevete

Este mai dificil să te ocupi de aceste tipuri de probleme etice. Un brevet poate păstra aspectul unic și secret al unei idei. Obținerea unui brevet este foarte dificil în comparație cu obținerea unui drept de autor. Este necesară o dezvăluire completă cu software-ul. Titularul

brevetului trebuie să dezvăluie detaliile complete ale unui program unui programator competent pentru construirea unui program.

Drepturi de autor

Specialiștii în securitatea informațiilor trebuie să fie familiarizați cu conceptul necesar al legii drepturilor de autor. Legea drepturilor de autor funcționează ca un instrument juridic foarte puternic în protejarea software-ului computerului, atât înainte de o încălcare a securității, cât și cu siguranță după o încălcare a securității. Acest tip de încălcare ar putea fi manipularea greșită și utilizarea incorectă a datelor, a programelor de computer, a documentației și a materialelor similare. În multe țări, legislația privind drepturile de autor este modificată sau revizuită pentru a oferi legi explicite pentru protejarea programelor de computer.

Secretele comerciale

Secretele comerciale sunt, de asemenea, o problemă etică semnificativă în tehnologia informației. Un secret comercial asigură ceva de valoare și utilitate. Această lege protejează aspectele private ale ideilor, care sunt cunoscute doar de descoperitor sau de confidentele sale. Odată dezvăluit, secretul comercial se pierde ca atare și este protejat de lege numai pentru secretele comerciale. Aplicarea legii secretului comercial este foarte largă în domeniul computerelor, unde chiar și un avans ușor în avansarea software-ului sau hardware-ului poate oferi o influență competitivă semnificativă.

Răspunderea

Ar trebui să fim conștienți de problema răspunderii în luarea deciziilor etice. Dezvoltatorul de software face promisiuni și afirmații utilizatorului cu privire la natura și calitatea produsului care pot fi restricționate ca garanție expresă. Programatorii sau comercianții cu amănuntul au legitimitatea de a stabili garanțiile exprese. Astfel, ele trebuie să fie practice atunci când definesc orice afirmații și predicții cu privire la capacitățile, calitatea și natura software-ului sau hardware-ului lor. Fiecare cuvânt pe care îl spun despre produsul lor poate fi valabil din punct de vedere juridic, așa cum este menționat în scris. Toate acordurile ar trebui să fie scrise pentru a se proteja împotriva răspunderii. O declinare a garanțiilor exprese poate elibera un furnizor de a fi tras la răspundere pentru declarațiile informale, speculative sau previziunile făcute în timpul etapelor acordului.

Pirateria

Pirateria este o activitate în care se face crearea de copii ilegale ale software-ului. Depinde în totalitate de proprietarul software-ului dacă utilizatorii pot face sau nu copii de rezervă ale software-ului lor. Pe măsură ce legile făcute pentru protecția drepturilor de autor se dezvoltă, este luată în considerare și legislația care ar opri duplicarea neautorizată a software-ului. Industria software-ului este pregătită să se confrunte cu pirateria software-ului. Instanțele se ocupă cu un număr tot mai mare de acțiuni privind protecția software-ului.

Concluzie

Un profesionist IT are obligația suplimentară de a raporta orice semn de risc al sistemului care ar putea provoca daune. Dacă cei responsabili nu acționează pentru a reduce sau a atenua aceste riscuri, poate fi necesar să trageți alarma pentru a reduce potențialul rău.

Cu toate acestea, informațiile înșelătoare sau înșelătoare despre riscurile potențiale pot fi dăunătoare. Înainte de a raporta riscurile, un profesionist IT trebuie să evalueze cu atenție aspectele relevante ale situației. Profesioniștii în informatică trebuie să evalueze dacă rezultatele eforturilor lor vor respecta diversitatea, dacă vor fi utilizate într-o manieră responsabilă din punct de vedere social, satisfăcând nevoile sociale și dacă vor fi accesibile pe scară largă. Aceștia sunt încurajați să contribuie activ la societate prin muncă voluntară și altruistă care aduce beneficii binelui public. Pe lângă un mediu social sigur, bunăstarea umană necesită un mediu natural sigur. Prin urmare, profesioniștii IT ar trebui să promoveze sustenabilitatea mediului atât local, cât și global.

Bibliografie

<https://www.rep.routledge.com/articles/thematic/information-technology-and-ethics/v-1#:~:text=Information%20technology%20ethics%20is%20the,moral%20underpinnings%20of%20public%20policy.>

<https://www.computerworld.com/article/2557944/ethical-issues-for-it-security-professionals.html>

<http://www.it.uu.se/research/project/itethics>

<https://er.educause.edu/articles/2017/3/ethics-and-the-it-professional>

<https://www.geeksforgeeks.org/ethical-issues-in-information-technology-it/>

<https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/ethics-in-information-technology>

<https://www.acm.org/about-acm/code-of-ethics-in-spanish>

<https://www.uniassignment.com/essay-samples/information-technology/importance-of-ethics-among-the-it-professional-information-technology-essay.php>

<https://bizfluent.com/about-4743180-ethics-information-technology.html>

<https://www.reference.com/business-finance/importance-ethics-information-technology-aa2450ed890d3574>

<https://www.open.edu/openlearn/education/educational-technology-and-practice/educational-technology/introducing-ethics-information-and-computer-sciences/content-section-0>