LIANGROUP

Mehrna Rayaneh Lian

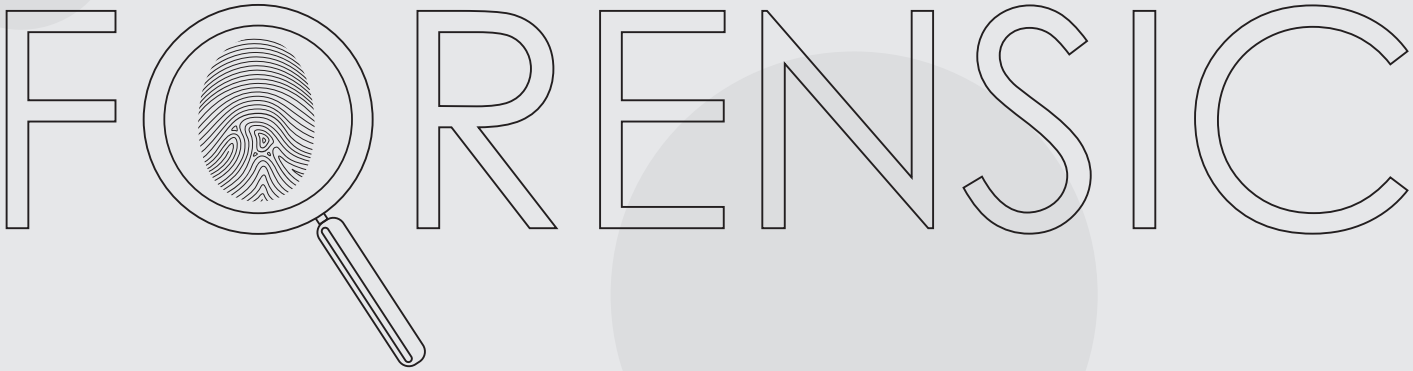
۰۲۱ ۹۱۰۰٤۱۵۱

تهران، فلکه دوم صادقیه، بلوار آیت الله کاشانی

خ نجف زاده فروتن، خ اعتمادیان، پلاک ٤۲، واحد ۲

www.liangroup.net

برای مدیران شرکت‌های مختلف مهم و حیاتی می‌باشد که با دانستن نقش سیستم‌های رایانه‌ای و شبکه‌ها و تاثیر آن‌ها بر عملکرد بخش‌های مختلف شرکت‌های خود آشنا باشند تا بتوانند بر ضرورت خطرهای حاصله از جرایم رایانه‌ای و چگونگی مقابله با خطراتی ازاین دست آگاهی لازم را داشته باشند. مدیران شبکه و کارمندان نهادهای امنیت مجازی بایستی از انواع خطرات و جرایم رایانه‌ای اطلاع کافی داشته باشند. این افراد می‌توانند در شرکت‌های دولتی حقوقی و یا خصوصی مشغول فعالیت باشند و این دسته از افراد بایستی با داشتن دانش کافی بتوانند برای حفظ امنیت داده‌های شرکت‌های خود اقدامات لازم را در دستور کار قرار دهند.



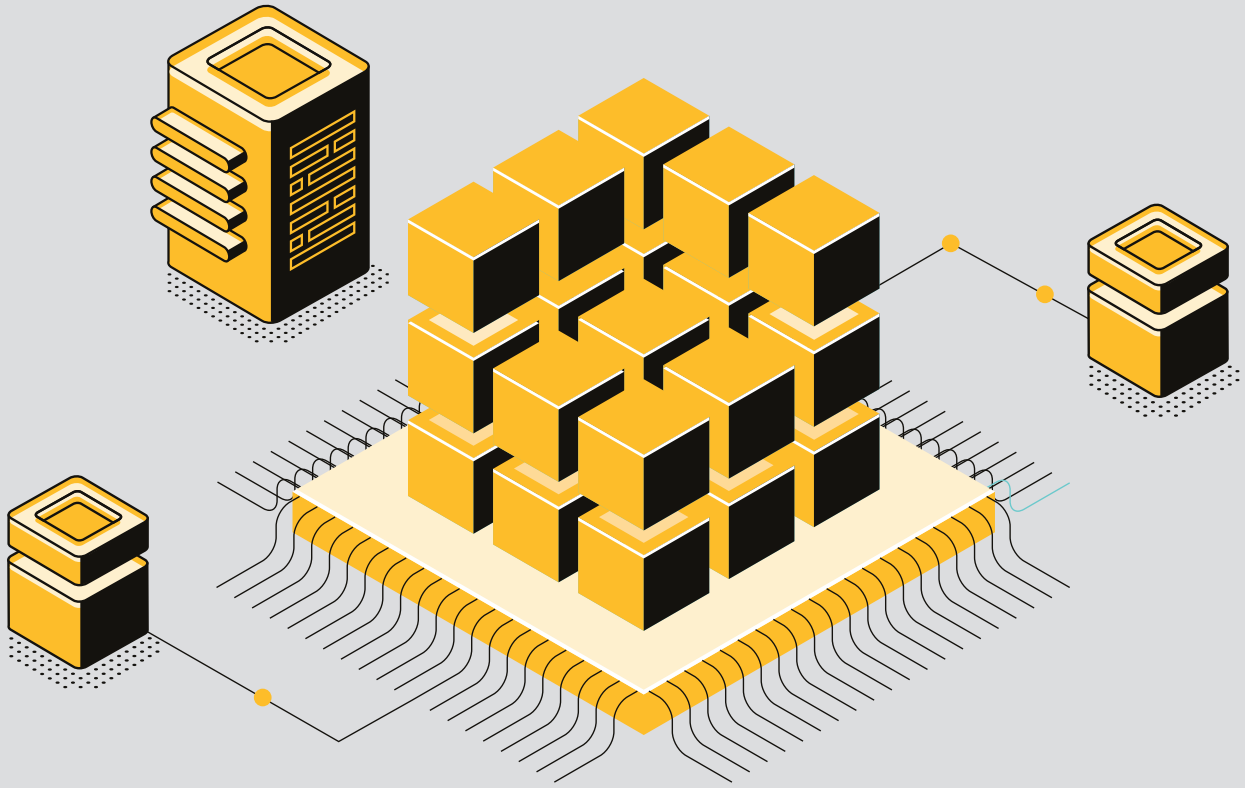
جرایم رایانه ای چیست؟

اگر شما یک مدیر شبکه هستید یا اینکه در حال استفاده از حتی یک رایانه ساده شخصی می‌باشید، بایستی بدانید که جرایم رایانه‌ای شامل چه مواردی می‌شود. واژه Forensic که بعضا از آن به عنوان دفاع رایانه‌ای یاد می‌شود در واقع فرآیندی است که شامل جمع آوری اطلاعات تحلیل و بررسی اطلاعات باقیمانده از یک مثلا نفوذ غیر قانونی به شبکه شما و یا هرشرکتی، برای ارائه به دادگاه انجام می گیرد. معنی لغوی Forensic یعنی ارائه مستندات به دادگاه.

چرا جرایم رایانه ای و راه های مقابله با آن ها تحت عنوان Forensic مهم است؟

افزودن قابلیت دفاع در برابر خطرات رایانه ای می تواند منجر به اطمینان بخشی به کاربران و افزایش توانایی شکست ناپذیری شبکه شما را در مقابل حملات سایبری به همراه داشته باشد. می توان برای شرکت ها به عنوان اولین قدم در راستای افزایش امنیت و راه اندازی سیستم های امنیتی از راهکار Defense -in-depth استفاده نمود. دراین فرآیند اگر شبکه و یا سیستم های کامپیوتری شما دچار نفوذ شد از قبل با امن سازی اطلاعات حیاتی شرکت خود هم می توانید از ضررهای مالی پیش رو جلوگیری کنید و هم اینکه می توانید اقدام به جمع اوری اطلاعات لازم برای ارائه به دادگاه و اقامه دعوی نمایید تا بتوانید فرد مهاجم را دستگیر کنید. به راستی اگر شما فرآیند امن سازی شبکه ای خود را انجام ندهید و یا در صورت انجام آن را اشتباه تنظیم نمایید چه اتفاقی خواهد افتاد؟ با این اشتباه شما هم ریسک ضررکرد مالی بسیار برای شرکت خود و همچنین خطر نشت اطلاعات حساس و استراتژیک شرکت را به جان خریده اید و هم اینکه مدارک لازم برای ارائه به دادگاه را نخواهید داشت. دراین حالت بدلیل اینکه شما و یا شرکت تان نتوانسته اید به درستی از اطلاعات محافظت کنید ممکن است که خودتان نیز به سهل انگاری در حفظ اطلاعات کاربران متهم شوید زیرا که شرکت شما و یا شخص شما بدلیل تنظیم یکسری دستورات اشتباه حتی سهوا نیز از دید دادگاه متخلف بوده و یا اینکه ممکن است به اتهام همدستی با فرد نفوذگر متهم شوید.

در واقع فرآیند
جمع آوری مدارک برای ارائه به
دادگاه یا Forensic می تواند شامل اثر
انگشت فرد بر روی مانیتور یا پنجره تا حتی
تشخیص نوع DNA باقیمانده متهم، حاصل
ازعمل خلاف قانون فرد مذکور باشد.



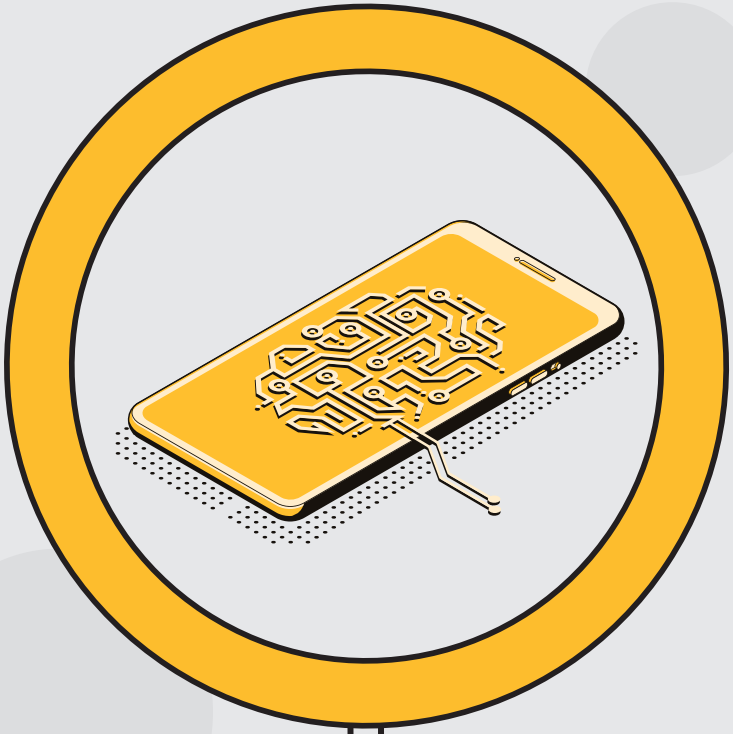
دو دسته اطلاعات در فرآیند جمع آوری اطلاعات مورد بررسی قرار می گیرند :

اطلاعاتی که به آن ها اطلاعات نوع President می گویند که شامل اطلاعاتی می شود که بر روی هارد کامپیوتر و یا فلش مموری یا هر دستگاه دیگری که اکنون خاموش است و توسط کاربران مختلف در محیط های مختلف مورد استفاده می باشد، ذخیره شده است و در زمانی که سیستم او خاموش است این اطلاعات نیز به طبع در دسترس نمی باشد.

نوع دیگر اطلاعات Volatile می باشد که در واقع به اطلاعاتی اطلاق می شود که برروی حافظه رم رایانه ذخیره شده است و اکنون در حال کار است و در صورت برق رفتگی یا ریستارت شدن سیستم از بین می رود. از آنجایی که اطلاعات در رم یا دیگر قسمت های سیستم همچون کش CPU به راحتی از بین می رود، بسیار ضروری است که قبل از بین رفتن اطلاعات، اقدام به جمع آوری اطلاعات کرد. نکته مهم این است که سیستم ها نباید خاموش و یا ریستارت شوند.

جنبه های قانونی فرایند
جمع آوری اطلاعات برای ارائه به دادگاه :

هرکس که در زمینه امنیت شبکه درحال کار می باشد بایستی به فعالیت های قانونی و فرآیندهای جمع آوری اطلاعات برای ارائه به دادگاه آگاهی کافی را داشته باشد. مسئولین امنیتی شرکت های مختلف بایستی با تصمیم گیری های صحیح و تنظیم فرآیندهای امنیتی مفید به پیشبرد راه های مقابله قانونی با متهمان کمک بنمایند. به عنوان مثال حتی اگر دانش لازم برای جمع‌آوری اطلاعات به دادگاه را دارید باید قبل از شروع به هر اقدامی مجوزهای قانونی لازم را اخذ نمایید. ابزارهای زیادی برای جستجوهای لازم و جمع آوری اطلاعات وجود دارد که حتی بعضا استفاده از آن ها می تواند غیر مجاز باشد.



زمینه های مختلف
علم فارنزیک دیجیتال
عبارتند از :

- فارنزیک کامپیوتر
- فارنزیک موبایل
- فارنزیک شبکه
- فارنزیک بد افزارها