هرم DIWK یا هرم دانش

برای استخراج دانش از داده های خام نیاز است که داده ها پردازش شوند. مراحل پردازش داده ها به صورت کلی در هرم دانش خلاصه می‌شود. هرم دانش، سلسله مراتب خِرد و سلسله مراتب اطلاعات بعضی از نام هایی هستند که به نمایش روابط بین داده‌ها، اطلاعات، دانش و خرد اشاره می‌کند.

هرم دانش نیز همانند مدل های سلسله مراتبی دیگر از مجموعه بلوک هایی ساخته شده که ترتیب دارد. داده‌ها (data) در پایین ترین قسمت پس از آن اطلاعات (information) و سپس دانش (knowledge) قرار می‌گیرند و بالاترین بخش این هرم خرد (wisdom) است.

هر مرحله‌ای که در این هرم طی می شود؛ به سوالی درباره‌ی داده های اولیه پاسخ داده و به آن ارزش هایی اضافه می‌شود. هرچقدر به سوالات بیشتری پاسخ داده بشود مراحل بیشتری در این هرم طی خواهد شد. به بیانی دیگر هرچه معنای بیشتری از داده ها استخراج کنیم، به دانش و بینش بیشتری از داده های اولیه دست یافته‌ایم. در راس هرم، ما دانش و بینش ها را به یک تجربه یادگیری تبدیل کرده‌ایم که راهنمای اعمال ما است.

در ادامه بخش های مختلف هرم داده را بررسی می‌کنیم:

۱. داده ها

داده ها مجموعه‌ای از حقایق به صورت خام یا سازمان یافته مانند اعداد یا حروف هستند.

به هرحال بدون داشتن متن(متغیر)، داده ها ممکنه معنی کمی داشته باشند. برای مثال ۱۴۰۱۱۱۱۰ فقط توالی اعداد است که اهمیت آشکاری ندارند. اما اگر ما آن را در متن «این یک تاریخ است» مشاهده کنیم؛ آن گاه می‌توان گفت این توالی اعداد به معنی ۱۰ ام ماه بهمن سال ۱۴۰۱ است. با اضافه کردن متن و ارزش به این اعداد، آن ها معنی بیشتری نسبت به قبل دارند. به این ترتیب ما توالی خام اعداد را به اطلاعات تبدیل کرده‌ایم.

۲. اطلاعات

اطلاعات دومین بلوک ساختمانی هرم دانش است. در این مرحله داده ها از خطاها پاکسازی شده و بیشتر به روشی پردازش می‌شوند که اندازه گیری، تجسم و تجزیه و تحلیل برای یک هدف خاص رو آسان‌تر می‌کند.

بسته به این هدف، پردازش داده ها می‌تواند شامل عملیات مختلفی مانند ترکیب مجموعه های مختلف داده (جمع شدن)، اطمینان حاصل کردن از ارتباط و دقت داده های جمع آوری شده (اعتبار سنجی) و ... باشد. به عنوان یک مثال کلی، می‌توانیم داده های خودمان رو به گونه‌ای سامان دهیم که روابط بین نقاط مختلف داده های به ظاهر متفاوت و گسسته را در معرض نمایش قرار دهد.

با پرسیدن سوالات مرتبط با موضوع «چه کسی»، «چرا»، «چه موقع»، «کجا»، «چه زمانی» و ... می‌توانیم اطلاعات ارزشمندی از داده ها به دست آوریم و پاسخ این سوالات، داده ها را برای ما مفید تر می‌کند.

اما چه زمانی به سوال «چگونه» پاسخ دهیم؟ این همان چیزی است که باعث جهش از اطلاعات به دانش می‌شود.

۳. دانش

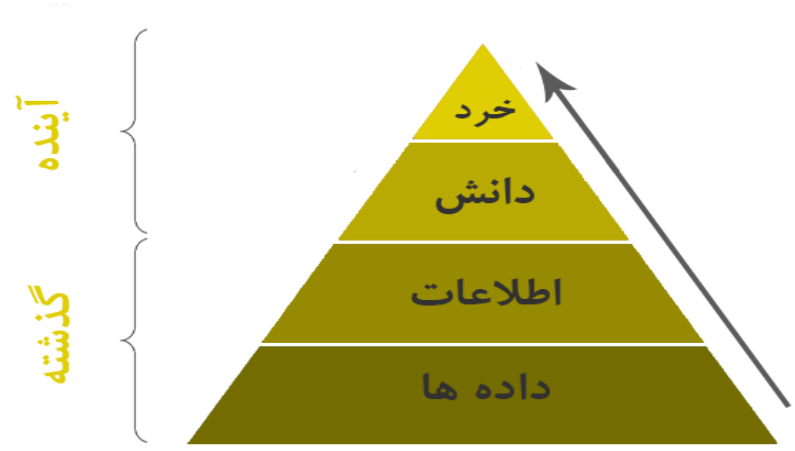
«چگونه» اطلاعات حاصل از داده های جمع آوری شده، مربوط به اهداف ما هستند؟ «چگونه» قطعات این اطلاعات به سایر قسمت ها متصل می‌شوند تا معنا و ارزش بیشتری بیابند؟ و شاید مهم ترین سوال در این بخش این باشد که:

«چگونه» می‌توانیم از اطلاعات برای دستیابی به هدف خود استفاده کنیم؟

هنگامی که ما اطلاعات را تنها به عنوان توضیحی از حقایق جمع آوری شده نمی‌بینیم و درک می‌کنیم که چگونه می‌توان از آن برای دستیابی به اهدافمان استفاده کرد، ما آن را به دانش تبدیل کرده‌ایم. این دانش اغلب برتری است که شرکت ها نسبت به سایر رقبای خود دارند. هرچه ما روابطی کشف کنیم که صریحاً به عنوان اطلاعات بیان نشده است، ما بینش های عمیق تری را بدست می‌آوریم که باعث می‌شود ما یک مرحله در هرم دانش بالاتر رویم. هنگامی که از دانش و بینش های به دست آمده از اطلاعات برای تصمیم گیری ها استفاده می‌کنیم، می توان گفت که ما به مرحله نهایی «خرد» از هرم دانش رسیده‌ایم.

٤. خرد

خرد بالاترین مرحله هرم دانش است و برای رسیدن به این مرحله باید به سوالاتی از قبیل «چرا کاری انجام دهیم؟» و «بهترین کار چیست؟» پاسخ دهیم. به عبارت دیگر، خرد دانشی است که در عمل به کار برده می‌شود. همچنین می‌توان گفت اگر مرحله داده ها و اطلاعات شبیه به نگاه کردن به گذشته باشند، مراحل دانش و خرد به این مربوط می‌شود که ما در حال حاضر برای بهتر شدن آینده، چه کاری می‌توانیم انجام دهیم.



مفهوم داده

مفهوم داده در زمینه محاسبات ریشه در کار کلود شانون، ریاضیدان آمریکایی معروف به پدر نظریه اطلاعات دارد. او مفاهیم دیجیتالی دودویی را بر اساس اعمال منطق بولی دو ارزشی برای مدارهای الکترونیکی مطرح کرد. فرمت‌های دو رقمی زیر بنای CPUها، حافظه‌های نیمه‌هادی و درایوهای دیسک، و همچنین بسیاری از دستگاه‌های جانبی رایج امروزه در محاسبات است. ورودی اولیه رایانه هم برای کنترل و هم برای DATA ها به صورت کارت‌های پانچ و سپس نوار مغناطیسی و هارد دیسک بود. در اوایل، اهمیت DATA ها در محاسبات تجاری با محبوبیت اصطلاحات «پردازش داده» و «پردازش داده های الکترونیکی» آشکار شد که برای مدتی طیف وسیعی از آنچه امروزه به عنوان فناوری اطلاعات شناخته می‌شود را شامل می‌شود.

نحوه ذخیره اطلاعات

کامپیوترها داده ها، از جمله ویدئو، تصاویر، صداها و متن را به عنوان مقادیر دودویی با استفاده از الگوهای عددی ۱ و ۰ نشان می‌دهند. بیت کوچکترین واحد دیتا است و فقط یک مقدار واحد را نشان می‌دهد. یک بایت هشت رقم دوتایی است .حافظه بر حسب مگابایت و گیگابایت اندازه‌گیری می‌شود. با افزایش حجم داده های جمع‌آوری شده و ذخیره شده، واحدهای اندازه‌گیری داده ها همچنان در حال رشد هستند. به عنوان مثال، عبارت نسبتاً جدید brontobyte ذخیره داده است که برابر با ۱۰ تا ۲۷ قدرت بایت است. داده ها را می‌توان در قالب‌های فایل ذخیره کرد، مانند سیستم‌های اصلی با استفاده از ISAM وVSAM. سایر فرمت‌های فایل برای ذخیره، تبدیل و پردازش داده ها شامل مقادیر جدا شده با کاما است. این فرمت‌ها همچنان در انواع مختلف ماشین‌ها کاربرد پیدا می‌کردند، حتی در حالی که رویکردهای ساختارمندتر داده محور در محاسبات شرکتی جای خود را پیدا کردند. تخصص بیشتر به عنوان پایگاه داده، سیستم مدیریت پایگاه داده و سپس فناوری پایگاه داده رابطه‌ای برای سازماندهی اطلاعات ایجاد شد. محدوده اندازه‌گیری داده ها. دامنه داده های دیجیتالی در طول زمان از بیت و بایت به brontobytes تبدیل شده است و اندازه‌گیری داده های بزرگتر در آینده در راه است.

مفاهیم اصلی در امنیت پایگاه داده کدامند؟

به طور کلی، امنیت پایگاه داده سه مفهوم کلیدی را در بر می‌گیرد که در ادامه به آن‌ها پرداخته می‌شود:

1. *محرمانگی در امنیت پایگاه داده*

در مفاهیم امنیت پایگاه داده، «حفظ محرمانگی اطلاعات (Confidentiality) «به عنوان اولین معیار در نظر گرفته می‌شود. امکان ایجاد محرمانگی از طریق رمزنگاری داده‌های ذخیره شده در پایگاه داده امکان‌پذیر است. رمزنگاری یک روش یا فرآیندی است که در آن داده‌ها کدگذاری می‌شوند. این کدگذاری به گونه‌ای انجام می‌شود که تنها کاربران مجاز امکان خواندن داده‌ها را داشته باشند .به بیان دیگر، رمزنگاری یعنی داده‌های حساس برای کاربران غیرمجاز به صورت غیرقابل خواندن هستند. الگوریتم‌های رمزنگاری مختلفی مانند DES ، AES و Triple DES برای برقراری و حفظ محرمانگی در پایگاه داده استفاده می‌شوند.

۲. *تمامیت در امنیت پایگاه داده*

مفهوم تمامیت (Integrity) در امنیت پایگاه داده از طریق تنظیمات مربوط به کنترل‌های دسترسی کاربری (UAC) اعمال می‌شود. با استفاده از این مفهوم، به هر کاربر دسترسی به پایگاه داده تا سطح مورد نیاز داده خواهد شد. به عنوان مثال، ممکن است به یک کارمند اجازه دیدن رکوردها و تغییر بخش‌هایی از اطلاعات، مثل جزییات شماره تماس داده شود، اما کارمند بخش منابع انسانی دسترسی‌های بیش‌تری داشته باشد. برای اطمینان از تمامیت پایگاه داده روش‌هایی وجود دارند که در ادامه به آن پرداخته می‌شود:

- پس از نصب پایگاه داده، باید رمز عبور تغییر داده شود. علاوه بر این، بررسی‌های دوره‌ای گوناگونی لازم است تا این اطمینان به وجود بیاید که رمز عبور در خطر قرار نگرفته است.
- باید آن دسته از حساب‌های کاربری که استفاده نمی‌شوند، قفل شوند. در شرایطی که یک حساب کاربری به طور قطعی هیچ‌گاه دوباره استفاده نخواهد شد، بهترین اقدام حذف آن است.
- لازم است سیاست‌های پیشرفته مختلفی برای رمزهای عبور قوی ایجاد شوند. یکی از ایده‌های کارامد در این خصوص، الزام در تغییر رمز عبور به صورت ماهانه است.
- بررسی نقش‌ها و تنظیم دسترسی‌ها بر اساس آن‌ها بسیار اهمیت دارد. در واقع، باید این اطمینان حاصل شود که کاربران تنها به مواردی دسترسی دارند که مجاز به استفاده از آن‌ها هستند. با وجود اینکه بررسی این موضوع برای پایگاه داده‌های بزرگ بسیار زمان‌بر است، اما اگر دسترسی‌ها به درستی تنظیم شوند، ورود یا دسترسی غیرمجاز به راحتی قابل بررسی خواهد بود.
- بررسی اینکه آیا کسب و کار مربوطه چندین ادمین پایگاه داده دارد یا خیر؛ در صورتی که پاسخ این سوال مثبت باشد، بهتر است وظایف میان این مدیران پایگاه داده تقسیم شوند.

۳. *دسترسی پذیری در امنیت بانک اطلاعاتی*

در یک سیستم کارآمد، نباید پایگاه داده از کارافتادگی بازه‌ای داشته و نرخ دسترس پذیری (Availability) آن باید قابل قبول باشد. در واقع، برای جلوگیری از رخداد برنامه‌ریزی نشده چنین اتفاق‌هایی، می‌توان از اقدامات مختلفی استفاده کرد که در ادامه فهرست شده‌اند:

- محدود کردن میزان فضای ذخیره‌سازی برای کاربران در پایگاه داده
- ایجاد محدودیت در تعداد نشست‌های(Session) های (موازی قابل دسترسی برای هر کاربر پایگاه داده
- پشتیبانی‌گیری از داده‌ها به صورت دوره‌ای به منظور کسب قابلیت بازیابی داده در صورت بروز مشکلاتی در اپلیکیشن
- ایجاد ایمنی در پایگاه داده در برابر آسیب‌های امنیتی
- استفاده از پایگاه داده‌های خوشه‌ای با هدف افزایش دسترسی پذیری

مزیت‌های امنیت پایگاه داده

برقراری امنیت پایگاه داده یک اقدام ضروری در سازمان‌هایی است که دارای پایگاه‌های داده و سیستم‌های مدیریت پایگاه داده مرتبط با یکدیگر هستند. در این سازمان‌ها، اقدامات مربوط به برقراری امنیت پایگاه داده در کنار عناصر عملکردی برنامه‌های

کاربردی این سازمان‌ها مورد استفاده قرار می‌گیرند. در حقیقت، با به کارگیری اقدامات احتیاطی راه‌اندازی شده در جهت افزایش امنیت پایگاه داده می‌توان جلوگیری از بسیاری از عواقب احتمالی جدی نقض امنیت را تسهیل کرد. در ادامه برخی از ویژگی‌های مفید اجرای عناصر امنیت پایگاه داده فهرست شده‌اند:

- می‌توان پایگاه‌های داده را در برابر نقض‌های امنیتی و فعالیت‌های هک، از جمله نفوذ فایروال (Firewall Intrusion)، انتشار ویروس و باج افزار (Ransomware) محافظت کرد. اعمال اقدامات مربوط به امنیت پایگاه داده در نهایت محافظت از اطلاعات حساس شرکت را تسهیل می‌کند. بنابراین، در مواقع مختلفی که به هیچ دلیلی نمی‌توان اطلاعات را با افراد خارجی به اشتراک گذاشت، افزایش امنیت پایگاه داده بسیار مفید است.
- امکان توقف حملاتی مانند فایل‌های مسری بدافزار و سایر موارد مخربی فراهم می‌شود که ممکن است برای سیستم‌های پایگاه داده ناامنی ایجاد کنند.
- ارائه حفاظت تضمین شده برای سیستم‌های سرور فراهم می‌شود. بنابراین، امکان محافظت از این سیستم‌های سرور در برابر هر گونه آسیب قابل توجهی که منجر به شکست در پردازش یا بازیابی داده بشوند؛ وجود دارد.
- امنیت پایگاه داده با تعهد کاربران پایگاه داده و متخصصان مدیریت از حوزه کسب و کار همراه است تا داده‌های ادراکی را دقیقاً برای استفاده مناسب از اطلاعات جمع‌آوری کنند.
- زمانی که امنیت پایگاه داده با سیاست‌ها و شرایط شرکت مطابقت داشته باشند، اپلیکیشن‌ها از خطر خراب شدن عاری خواهند بود. به این دلیل که علاوه بر بهبود عملکرد سازمان با مقرون به صرفه‌تر کردن هزینه‌ها، از سازمان محافظت می‌کنند.
- با وجود اینکه افزودن ویژگی‌های جدید به امنیت پایگاه داده سازمان مربوطه برای کسب‌وکار هزینه‌زا است، اما با کمک این رویکرد، اطمینان حاصل می‌شود که هزینه‌ها به جای ضرر به سرمایه‌گذاری تبدیل خواهند شد.

کنترل‌های امنیتی برای برقراری امنیت پایگاه داده

انواع کنترل‌های امنیتی برای پایگاه داده در موقعیت های مختلف به شرح ذیل است:

۱. داده‌ها در حمل و نقل و کنترل دسترسی در امنیت پایگاه داده

به طور کلی، کنترل دسترسی (Access Control) داده‌ها در حمل و نقل، به سیستم امنیتی خاصی اطلاق می‌شود که با کمک آن، اطمینان لازم از فرآیند انتقال حاصل خواهد شد. به بیان ساده، با استفاده از این نوع کنترل امنیت پایگاه داده هیچکس نمی‌تواند داده‌ها را هنگام انتقال بین سرورهای مختلف یا پیکربندی شبکه‌ها بخواند یا تفسیر کند.

هدف اصلی در این نوع از امنیت پایگاه داده محدود کردن هرگونه گره (Node) بالقوه مربوط به رخنه یا دسترسی غیرمجاز به سیستم‌های سرور در هر زمانی است. بنابراین، این تنظیمات داده‌ها به عنوان کنترل دسترسی نیز شناخته می‌شوند. هر گره داده مشخصی که از سیستم سرور ایمن خارج و وارد آن می‌شود، کاملاً رمزنگاری شده و غیرقابل خواندن است. مگر اینکه به طور امن در پایگاه داده سیستم ایمن سپرده شود یا به کاربر درخواست کننده آن داده، نمایش داده شود.

برخی از سازمان‌ها یا شرکت‌ها با این موضوع موافق نیستند و بر غیرضروری بودن اجرای این مورد تاکید دارند. با این وجود، در عمل این اقدام یکی از اصلی‌ترین گام‌هایی است که در جهت افزایش امنیت پایگاه داده کاربرد دارد. در طول چند سال اخیر، این

مفاهیم در بهترین دوره‌های امنیت پایگاه داده متعددی نیز تدریس شده‌اند. این دوره‌ها برای پرسنل و متخصصانی اهمیت دارند که به عنوان کارشناس امنیت پایگاه داده و پیکربندی داده‌ها به دنبال مشاغل پرتقاضا هستند.

۲. احراز هویت در کنترل‌های امنیت در پایگاه داده

احراز هویت (Authentication) به عنوان مورد بعدی از انواع امنیت پایگاه داده مطرح می‌شود و پس از تکمیل داده‌ها، لازم است این موضوع در پروتکل حمل و نقل اعمال شود. این پروتکل امنیتی دارای لایه‌های مختلفی در درون خود است. به طور کلی، احراز هویت راهی است که از طریق آن تأیید می‌شود آیا کاربر همان شخصی است که می‌گوید یا خیر؟

به عبارت ساده‌تر، Authentication به معنی احراز هویت درخواست یا کوئری ارسال شده توسط پرسنل مجاز یا کاربر اختصاصی است. به منظور عملی کردن احراز هویت، می‌توان از روش‌های مختلفی استفاده کرد. به عنوان مثال، استفاده از روش احراز هویت چند عاملی (Multi-Factor) که در آن لایه‌های امنیتی مختلف به طور ترکیبی اضافه می‌شوند. این فرآیند منجر به احراز هویت یک کاربر خاص و موفقیت او در دسترسی می‌شود. در صورتی که فرآیند احراز هویت به عنوان یک عمل کاربردی در مورد پیکربندی و امنیت پایگاه داده اعمال نشود، هر کسی، حتی هکرهای غیرقانونی، به راحتی به سرورهای پایگاه داده دسترسی خواهند داشت و باعث خرابی و به مخاطره انداختن امنیت پایگاه داده می‌شوند. به منظور اعطای دسترسی و احراز هویت موثر کاربر، می‌توان از مواردی مانند احراز هویت دو مرحله‌ای (Two-Factor) و احراز هویت از طریق نام کاربری و رمز عبور استفاده کرد.

۳. صدور مجوز در کنترل‌ها امنیت پایگاه داده

مرحله بعدی در این فرآیند و نوع سوم حفظ امنیت پایگاه داده ، صدور مجوز (Authorization) است. با به کارگیری این لایه امنیتی، مشخص می‌شود که کاربر اختصاصی (Dedicated) دقیقاً به چه عناصری دسترسی دارد. در صورت لزوم، می‌توان محدودیت‌هایی را برای یک کاربر مشخص اعمال کرد و دسترسی او تنها به یک نمای کلی از سیستم‌ها محدود شود. به عنوان مثال، ممکن است یک کاربر به محتوای کلی وب سایت دسترسی داشته باشد، اما اطلاعات محرمانه پراهمیتی مانند اطلاعات شخصی یا مالی سایر کاربران برای او یا هر کاربر Guest یا معمولی دیگری محدود شوند.

این مرحله از امنیت پایگاه داده از همه آن‌ها مهم‌تر است. چراکه به واسطه آن، اطمینان لازم برای برقراری امنیت پایگاه داده حاصل می‌شود. در حقیقت، با استفاده از Authorization هیچ‌کس نمی‌تواند به مناطق ناشناخته سرک بکشد یا بخش‌هایی را کاوش کند که قرار نیست مورد توجه آن‌ها قرار بگیرند. می‌توان سطح مجوز اختصاص داده شده به یک کاربر خاص را برای یک سازمان یا اپلیکیشن خاص، پیکربندی یا سفارشی‌سازی (Customized) کرد.

٤. داده‌ها در حالت استراحت

پس از به اشتراک گذاشتن یا در دسترس قرار گرفتن داده‌ها توسط کاربر، این داده‌ها در سرور باقی می‌مانند. این شرایط با نام «داده‌ها در حالت استراحت (Data At Rest) «در نظر گرفته می‌شوند. لازم به ذکر است که حتی پس از خاموش شدن سرور، داده‌ها همچنان باقی می‌مانند. برای این وضعیت، فناوری‌های رمزنگاری منحصر به فردی به کار گرفته شده‌اند که اطمینان حاصل می‌کنند داده‌ها حتی زمانی که از دسترس خارج شده‌اند، همچنان به صورت رمزنگاری شده خواهند بود.

۵. ممیزی و حسابرسی در امنیت پایگاه داده

با وجود اینکه هک و دسترسی غیرمجاز اهمیت بسیار زیادی دارد، اما این هک‌ها همچنان رخ می‌دهند و نمی‌توان هیچ کاری را در این زمینه انجام داد .بنابراین، پرداختن به امور ممیزی (Auditing) و حسابرسی سیستم بسیار حیاتی است. چون با کمک ممیزی می‌توان مطمئن شد که چه مواردی در خزانه (Inventory) وجود دارند. به عنوان مثال، آگاهی از اطلاعات ظریفی که در تلاش‌هایی برای هک کردن از دست رفته‌اند، یک ضرورت بخ حساب می‌آید. از این رو، باید گزارش‌گیری‌های ممیزی به طور مستمر انجام شوند تا اطمینان حاصل شود که سوابق مناسبی از همه موارد سیستم وجود دارند.

۶. بازیابی در امنیت پایگاه داده

علاوه بر موارد موثر در امنیت پایگاه داده مذکور، بازیابی (Recovery) نیز به عنوان یک سیستم اولیه در نظر گرفته می‌شود که به امنیت پایگاه داده مرتبط است. در واقع، تهیه نسخه‌های پشتیبان از داده‌هایی که در پایگاه داده ذخیره می‌شوند یک امر ضروری به حساب می‌آید. چون در صورت رخنه یا هک سیستم توسط هکر، با کمک این رویکرد سیستم مربوطه به طور کامل از بین نمی‌رود .علاوه بر این، باید این اطمینان حاصل شود که فایل‌های پشتیبانی کاملاً رمزنگاری شده و ایمن و دو نسخه از آن‌ها در مکان‌های مختلف موجود هستند.

رایج‌ترین مشکلات در امنیت پایگاه داده

شرایطی مختلفی وجود دارند که ممکن است هکرها به سازمان‌ها و اطلاعات شخصی مشتریان آن‌ها دسترسی غیرمجاز پیدا کنند. به عنوان مثال، در طول چند سال گذشته، در برخی از شرکت‌های مهم و سرشناس، از جمله Slack، یاهو و Equifax، نقض داده‌ها رخ داده است. این فعالیت‌های فراگیر تقاضا برای نرم افزار امنیت سایبری و تست وب اپلیکیشن را بیش از پیش افزایش داده‌اند. در حقیقت این ابزارها با هدف محافظت از داده‌هایی طراحی شده‌اند که افراد با کسب و کارهای آنلاین به اشتراک می‌گذارند.

در صورتی که این اقدامات امنیتی به کار برده شوند، دسترسی هکرها به تمام رکوردها و اسناد موجود در پایگاه داده‌ها، غیرمجاز خواهد شد. علاوه بر این، با تطابق دادن قوانین با «مقررات عمومی حفاظت از داده‌ها عمومی (GDPR) «مراقبت و حافظت از داده‌های کاربری به مراتب قدرتمندتر می‌شود. در این بخش از مطلب «امنیت پایگاه داده چیست»، به انواع آسیب‌پذیری‌های رایجی پرداخته می‌شود که در سیستم‌های مبتنی بر پایگاه داده مشاهده شده است .علاوه بر این، در ادامه راه‌هایی برای رفع این مشکلات امنیت پایگاه داده ارائه خواهد شد.

۱. عدم انجام تست امنیت پیش از مرحله استقرار

یکی از رایج‌ترین دلایلی که منجر به ضعیف شدن امنیت پایگاه داده می‌شود، عدم توجه به مرحله استقرار (Deployment) در فرآیند توسعه است. با وجود اینکه تست کارکرد (Functional Testing) به منظور کسب اطمینان از کارایی نهایی اعمال می‌شود، اما در صورت انجام عمل غیرمجاز توسط پایگاه داده، این نوع از تست امکان نمایش آن را نخواهد داشت. به همین دلیل، پیش از استقرار، بررسی امنیت وب سایت با انواع تست‌ها حائز اهمیت بسیاری است.

۲. رمزنگاری ضعیف و نفوذ داده‌ها در کنار یکدیگر

ممکن است برخی، پایگاه داده را به عنوان بخش بک اند (Back End) تنظیمات در نظر داشته باشند و تمرکز اصلی را روی حذف خطرهایی بگذارند که از اینترنت حاصل می‌شوند. در حالی که این چنین نیست. رابط‌های اینترنت مختلفی درون پایگاه داده هستند که در صورت وجود ضعف امنیتی، به راحتی امکان پیگیری آن‌ها توسط هکرها ایجاد می‌شود. به منظور جلوگیری از چنین شرایطی، استفاده از پلتفرم‌های ارتباطی رمزنگاری، از جمله SSL و TLS ضروری به حساب می‌آیند.

۳. ضعف در امنیت سایبری و به دنبال آن، پایگاه داده درهم شکسته

برای درک این مشکل امنیت پایگاه داده ، می‌توان به نقض داده‌های شرکت Equifax اشاره کرد. نمایندگان این سازمان اقرار کردند که داده‌های مربوط به ۱۴۷ میلیون مشتری در خطر افتاده بودند. بدیهی است که در چنین شرایطی، تبعات این ضعف امنیت پایگاه داده در سطح بسیار وسیعی باشد. در واقع، با توجه به این نمونه، اهمیت بیش از اندازه نرم افزار امنیت سایبری و نقش آن در حافظت از امنیت پایگاه داده به طور کامل نمایان می‌شود. متاسفانه به دلیل کمبود منابع یا زمان، اغلب کسب و کارها به عمل تست امنیت شبکه کاربر نمی‌پردازند و در سیستم‌های خود از Patch های دارای نظم استفاده نمی‌کنند .این موضوع باعث می‌شود که این کسب و کارها و امنیت پایگاه داده آن‌ها مستعد نشت داده‌ها (Data Leak) شوند.

٤. دزدیده شدن نسخه‌های پشتیبانی پایگاه‌های داده

به طور کلی، دو نوع خطر وجود دارند که به عنوان تهدید برای امنیت پایگاه داده شناخته می‌شوند. این تهدیدها در دو حالت خارجی و داخلی هستند. در برخی از مواقع، یک کسب و کار تهدیدهای داخلی متعددی را، حتی بیش‌تر از تهدیدهای خارجی، متحمل می‌شود. در حقیقت، هر اندازه که کارمندهای یک کسب و کار مسئولیت‌پذیر باشند و حتی، اگر هر نرم افزار امنیتی قابل قبولی استفاده شود، همچنان سازمان‌ها هیچ گاه نمی‌توانند به طور قطعی و صد در صدی از وفاداری کارمندان خود اطمینان حاصل کنند. چون هر شخصی که امکان دسترسی به داده‌های حساس و پراهمیت را دارد، می‌تواند به راحتی اطلاعات را دزیده و در جهت منافع خود، آن‌ها را به یک سازمان شخص ثالث بفروشد.

با این وجود، می‌توان با کمک اقدامات خاصی چنین ریسک‌هایی را حذف کرد یا به حداقل رساند. به منظور افزایش امنیت پایگاه داده و بهبود مشکل مذکور، مواردی مانند رمزنگاری آرشیوهای پایگاه داده، پیاده‌سازی استانداردهای امنیتی محکم، اعمال جریمه در صورت تخطی از قوانین و استفاده از نرم افزار امنیت سایبری به کار می‌روند. علاوه بر موارد ذکر شده، لازم است به طور مداوم با افزایش آگاهی تیم کاری از جلسه‌های سازمان، امنیت پایگاه داده را افزایش و ریسک در خطر قرار گرفتن آن را کاهش داد.

٥. وجود ضعف در ویژگی‌ها به عنوان یک مشکل امنیت پایگاه داده

در صورتی که درون ویژگی‌های پایگاه‌های داده ضعف‌های خاصی وجود داشته باشند، زمینه هک شدن آن‌ها توسط هکرها ایجاد خواهد شد. اساساً، هکرها می‌توانند اطلاعات کاربری و اعتبارات مربوطه را بشکنند و سیستم را وادار به اجرای هر کد دلخواهی کنند. با وجود اینکه این موضوع بسیار پیچیده به نظر می‌رسد، اما در واقع، این دسترسی‌ها از طریق ضعف‌های پایه مربوط به ویژگی‌های پایگاه‌های داده بدست می‌آیند. برای رفع این مشکل، می‌توان با تست امنیت پایگاه داده، Data ها را از دسترسی

شخص ثالث حفظ کرد و بدین طریق امنیت پایگاه داده را تا حدی افزایش داد. علاوه بر این، هر چه ساختار کارکرد پایگاه داده ساده‌تر طراحی شود، احتمال اینکه ویژگی‌های پایگاه داده به طور مطلوب محافظت شوند بیش‌تر می‌شود.

۶. زیرساخت پیچیده و ضعیف پایگاه داده

به طور کلی، معمولاً هکرها در یک عملیات، تمام پایگاه داده را تحت کنترل خود در نمی‌آورند. به بیان ساده، هکرها با هدف پیدا کردن یک ضعف خاص در زیرساخت پایگاه داده مربوطه و سو استفاده از آن عمل می‌کنند. هکرها یک رشته از حملات را اجرا می‌کنند و این عمل تا زمانی ادامه خواهد داشت که آن‌ها به بک اند دسترسی پیدا کنند. نرم افزار امنیت به طور کامل قابلیت محافظت از سیستم و چنین دستکاری‌هایی را دارا نیست.

حتی در شرایطی که به ضعف‌های ویژگی توجه شود، همچنان مهم است که زیر ساخت کلی پایگاه داده پیچیدگی بسیاری نداشته باشد. چون زمانی که زیرساخت پایگاه داده پیچیدگی زیادی دارد، این احتمال وجود دارد که برخی از نقاط ضعف بدون بررسی و رفع شدن، فراموش یا نادیده گرفته شوند. به همین دلیل، لازم است که همه بخش‌های سازمان مورد نظر به اندازه یکسان روی سیستم کنترل داشته باشند تا بدین طریق، تمرکز به صورت غیرمتمرکز باشد و ریسک‌های احتمالی به خطر افتادن امنیت پایگاه داده به حداقل برسند.

۷. دسترسی بدون محدودیت ادمین

تقسیم هوشمند وظایف میان ادمین و کاربر این اطمینان را ایجاد می‌کند که تنها افراد دارای تجربه کافی دسترسی بدون محدویت داشته باشند. با استفاده از این رویکرد، دیگر دزدیدن داده‌ها برای افرادی که در فرآیند مدیریت پایگاه داده مشارکت ندارند امری دشوار خواهد بود. حتی در صورتی که امکان محدود کردن تعداد حساب‌های کاربری وجود داشته باشد، معمولاً شرایط بهتر می‌شود. به این دلیل که در این شرایط، به دست گرفتن کنترل پایگاه داده توسط هکرها نیز با چالش‌های بیش‌تری همراه خواهد بود. می‌توان این موضوع را در کسب و کارهای مختلف اعمال کرد، اما معمولاً در صنعت مالی رخ می‌دهد. بنابراین، علاوه بر اینکه آگاهی از دسترسی افراد به داده‌های حساس مهم است، پیش از انتشار، مطلوب است که اجرای تست نرم افزار بانکداری نیز انجام شود.

۸. ناکافی بودن مدیریت کلید

با وجود اینکه رمزنگاری داده‌های حساس حائز اهمیت است، اما علاوه بر آن، توجه به اینکه دقیقاً چه افرادی به کلیدها دسترسی دارند نیز بسیار مهم به حساب می‌آید. با توجه به اینکه معمولاً کلیدها روی هارد دیسک یک فرد ذخیره می‌شوند، واضح است که از این طریق می‌توانند به آن‌ها دسترسی غیرمجاز پیدا کرد و به راحتی آن‌ها را دزدید. در واقع، اگر این ابزارهای مهم امنیت نرم افزار بدون حفاظت، نادیده گرفته شوند، در چنین شرایطی سیستم مورد نظر نسبت به حملات آسیب‌پذیر خواهد بود. بنابراین برای افزایش امنیت پایگاه داده ، لازم است به مدیریت کلیدها نیز توجه شود.

۹. بروز اختلالات در پایگاه‌های داده

یکی از مواردی که منجر به آسیب‌پذیری و به خطر افتادن امنیت پایگاه داده می‌شود، وجود ناسازگاری است. از این رو، لازم است تست امنیت وب سایت به طور مداوم انجام شود تا این اطمینان حاصل شود که داده‌ها حافظت خواهند شد. در شرایطی که

مغایرت در سیستم مشاهده شود، باید در اسرع وقت این مغایرت‌ها رفع شوند. در حقیقت، بهتر است توسعه دهندگان سازمان مورد نظر از هر گونه تهدید احتمالی آگاه باشند. تا بدین طریق، از اثرگذاری این تهدیدهای احتمالی روی دیتابیس و کاهش امنیت پایگاه داده جلوگیری کنند. با وجود اینکه نمی‌توان این کار را به راحتی انجام داد، اما با پیگیری‌های مداوم، امکان مخفی نگه داشتن اطلاعات و حفاظت آن‌ها وجود دارد.

امروزه، اغلب کسب و کارها آگاهی کافی در مورد اهمیت تست امنیت و ضرورت وجود آن را دارند. با این وجود، در بسیاری از سازمان‌ها تست امنیت پیاده‌سازی نمی‌شود. این موضوع یک اشتباه محض است که در طول مراحل توسعه بیش‌تر از همیشه نمایان می‌شود. البته باید توجه کرد که در مراحلی مانند ادغام برنامه کاربردی یا به روزرسانی پایگاه داده نیز، اهمیت پیاده‌سازی تست امنیت به صورت کامل قابل مشاهده است. مجرمان سایبری از این مشکلات در جهت منافع خود سو استفاده می‌کنند و در نتیجه، کسب و کار مربوطه ریسک‌های متعددی را متحمل خواهد شد.

بکاپ گیری

به فرآیند ذخیره و کپی کردن اطلاعات از کامپیوتر، سرور، موبایل و کلا هر دستگاه ذخیره‌ساز اطلاعات که بروی هارد و حافظه‌ی دستگاه ذخیره شده در هارد اکسترنال یا سایر دستگاه‌های ذخیره‌سازی اطلاعات، بکاپ گفته می‌شود. اطلاعات ممکن است شامل فیلم‌ها، عکس‌ها، آهنگ‌ها، فایل‌ها و سایر اسناد شخصی و سازمانی باشد. فرآیند بکاپ گیری باید به صورت منظم انجام شود زیرا گاهی **تعمیر هارد** کامپیوتر و ریکاوری اطلاعات آن به سختی انجام می‌شود.

چرایی تهیه بک‌آپ از اطلاعات

جواب واضح است، با **خراب شدن هارد و عدم شناسایی آن توسط سیستم** شما می‌توانید بر روی هارد جدیدی سیستم عامل و برنامه‌های خود را دوباره نصب کنید. اما بازیابی اطلاعات شخصی غیرممکن است، گاهی اوقات هم بر اثر اشتباهات انسانی و اتفاقات غیرمنتظره ممکن است بخشی یا کل اطلاعاتمان از بین برود. به همین دلیل است که شما باید از اطلاعات شخصی خود بک‌آپ بگیرید.

باید به صورت مداوم از **اسناد شخصی - کاری**، **تصاویر**، **ویدئوهای خانگی** و هر اطلاعات مهمی که بر روی کامپیوتر خود دارید بکاپ بگیرید، چون که آن‌ها اطلاعات غیرقابل جایگزینی هستند. اگر شما وقت زیادی را صرف گلچین کردن آهنگ‌ها و فیلم‌ها از CD و DVD ها کرده باشید شاید لازم باشد از این اطلاعات هم بک‌آپ بگیرید تا دوباره مجبور نباشید برای جمع آوری آن‌ها وقت بگذارید.

از سیستم عامل، برنامه‌ها و تنظیمات دیگر نیز می‌توانید پکاپ بگیرید. جا دارد که بگویم لازم نیست که از همه چیز بکاپ داشته باشید، اما هنگامی که مشکلی پیش بیاید شما می‌توانید به راحتی آن‌ها را بازگردانید کنید. اگر شما از آن دسته افراد هستید که دوست دارید با فایل‌های سیستمی و قسمت رجیستری کامپیوتر خود خیلی کار کنید و یا منظم سخت‌افزار خود را به روزرسانی کنید، هنگامی که مشکلی به میان می‌آید داشتن یک بکاپ کامل در وقت شما خیلی صرفه‌جویی می‌کند.

گاهی در اثر اتفاقات خواسته یا ناخواسته، به هر دلیلی ممکنه برای اطلاعات شما خسارات جبران ناپذیری رقم بخوره که داشتن یک بکاپ اطلاعاتی خوب، شما را در برابر هر خطری بیمه می‌کنه و به سرعت می‌توانید دوباره اطلاعات خود را جایگزین کنید. برخی دلایلی که ممکنه برای شما پیش بیاد تا دسترسی به اطلاعات خود نداشته باشید:

- عدم شناسایی هارد به دلیل آسیب‌های فیزیکی
- پاک کردن اطلاعات در اثر فرمت
- بدسکتوری شدن هارد دیسک
- از بین رفتن پارتیشن‌ها در هنگام نصب ویندوز
- ویروسی شدن هارد و اطلاعات

۵ مزیت تهیه Backup از دیتا

کارشناسان توصیه می‌کنند که از قوانین {۱و۲و۳} پیروی کنید. ۳ نسخه از فایل‌های مهم را نگهداری کنید (۱ نسخه اصلی و ۲ نسخه پشتیبان). فایل‌ها را در دو نوع رسانه مختلف برای محافظت از انواع خطرات نگهداری کنید. **هزینه‌های بازیابی اطلاعات** ممکن است در مواردی گران تمام شود، لذا داشتن یک نسخه پشتیبان قوی، به شما این امکان را می‌دهد که اطلاعات خود را بدون نیاز به پرداخت هزینه‌ای بازیابی کنید.

ژاپنی‌ها یک مثالی دارند که اطلاعاتی که ۵ جا نباشد انگار اصلا وجود نداره!! مزایا پشتیبان گیری از اطلاعات به شرح ذیل است:

۱. **دسترسی سریع به پرونده ها و فایل ها**

از مهم ترین موارد در زمینه تهیه نسخه پشتیبان، سهولت در بازیابی فایل ها و داده ها است. هنگامی که از اطلاعات، بکاپ تهیه می کنید، این امکان را دارید تا در کمترین زمان ممکن به پرونده های خاص دسترسی پیدا کنید. اگر از سیستم ذخیره سازی کلود استفاده می کنید، نه تنها دسترسی شما به اطلاعات سریعتر خواهد بود، بلکه از هر مکانی تنها با اتصال به اینترنت می توانید به داده های مورد نظر دسترسی داشته باشید.

۲. **محافظت در برابر قطعی برق و بلایای طبیعی**

در برخی موارد، کامپیوترها و تجهیزات ذخیره سازی مانند سرور و استوریج در معرض آسیب هایی قرار خواهند گرفت که کنترل آنها از دست شما خارج است مانند؛ طوفان شدید، خاموشی های تصادفی و قطع برق که امکان تخریب درایوهای ذخیره سازی را ایجاد میکند. بهترین راه حل، تهیه بک آپ از اطلاعات به صورت منظم یا اجازه به سیستم برای پشتیبان گیری به صورت خودکار است. دیگر نگران قطعی برق و از دست رفتن اطلاعات مهم خود نخواهید بود.

۳. **نصب آنتی ویروس برای جلوگیری از سرقت اطلاعات**

بی شک از میزان تخریبی که ویروس های اینترنتی می توانند بر روی تجهیزات و داده ها ایجاد کنند مطلع هستید. میزان پیشرفت ویروس ها و پیشرفت در تاثیر گذاری تنها در عرض چند ساعت می توانند تمام اطلاعات شما را برای همیشه از بین ببرند. استفاده

از یک آنتی ویروس یکی از راه ها برای کاهش خطر تهدیدات ناشی از ویروس ها می باشد، اما در کنار آن حتما از اطلاعات خود backup تهیه کنید. زیرا با این کار امنیت اطلاعات خود را تضمین خواهید کرد.

٤. **محافظت در برابر خرابی هاردیسک ها**

دلایلی که منجر به خرابی hard drive می شود متنوع و زیاد است. برخی هارد دیسک ها در صورت فرسودگی یا آسیب دیدن دیدن دچار نقص می شوند، علاوه بر این، هارد دیسک ها در لحظه خراب نمی شوند، این خرابی در طول مدت زمان و به تدریج ایجاد می شود. اینکه به چه دلیل این خرابی ایجاد شده است مهم نیست، زیرا در هر حالت نتیجه آن از دست رفتن اطلاعات است.

٥. **بازیابی در صورت خرابی سیستم عامل**

بخش عظیمی از خرابیها در کامپیوترهای بزرگ و کوچک، خرابی OS می باشد که میتواند به دلایل مختلفی اتفاق بیافتد. برخی Operating System ها به دلیل تخصیص نادرست فضای حافظه از کار می افتند و برخی در نتیجه خرابی نرم افزار یا خطاهای متعدد اپلیکیشن ها، در اثر گذشت زمان می باشد. در هر صورت برای جلوگیری و به حداقل رساندن هزینه ای که خرابی سیستم عامل، به وجود می آورد، گرفتن بکاپ از اطلاعات ضروری است. از آنجایی که امروزه به تجهیزات و اطلاعات خود وابسته هستید منطقی نیست که از اطلاعات خود تنها یک نسخه بلکه چندین نسخه و به روش های مختلف، بکاپ تهیه کنید.

۵ نوع اصلی بکاپ گیری اطلاعات

۱. **Full Backup**

همانطور که از نام این روش پیداست، نسخه کپی اطلاعات به صورت کامل از تمامی مواردی که مهم تلقی می شوند و نباید از بین روند گرفته می شود. این نوع بکاپ اولین نسخه و به طور کلی معتبرترین نسخه است، زیرا بدون نیاز به ابزارهای جانبی و اضافه تهیه می شود.

۲. **Incremental Backup**

در این روش تهیه نسخه پشتیبان نیاز به دقت بیشتری می باشد، زیرا شامل تهیه کپی از File ها با در نظر گرفتن تغییراتی است که از زمان گرفتن نسخه بکاپ قبلی در آن اطلاعات ایجاد شده است. به عنوان مثال؛ تصور کنید یک نسخه بکاپ تهیه کرده اید، پس از اتمام کار، تصمیم می گیرید که به علت ادامه کار، بکاپ افزایشی را انجام داده و در این حالت دو نسخه ایجاد می شود. در روش Incremental تشخیص داده می شود که تمام پرونده های موجود در نسخه پشتیبان کامل، یکسان مانده و تنها نسخه بکاپ جدید را از فایل جدید ایجاد شده تهیه می کند. بنابراین بکاپ تکراری ایجاد نمی شود.

پشتیبان گیری افزایشی باعث صرفه جویی در وقت و فضای ذخیره سازی می شود، زیرا در صورت وجود full backup از قبل، همیشه تعداد فایل های کمتری برای تهیه بکاپ وجود دارد. توصیه می شود در این روش، از گرفتن Backup به صورت Manual (دستی) استفاده نشود. تنها مشکل موجود در زمان بازیابی اطلاعات است زیرا هم پیچیده تر است و هم نیاز به زمان بیشتر به علت سرعت پایین عملیات دارد. ابتدا آخرین نسخه بکاپ کامل بازیابی و سپس موارد افزایشی، اعمال میشود.

۳. **Reverse incremental Backup**

در روش Reversed incremental backup ابتدا یک نسخه بکاپ کامل از اطلاعات ایجاد می شود و بطور دوره ای این نسخه بکاپ را با live copy گرفته شده همسان سازی کرده و نسخه های قدیمی را بازسازی میکند. در صورت نیاز به Restore اطلاعات، نسخه های محدودی وجود دارند و کار پیچیده ای نیست.

٤. Differential Backup

این نوع نسخه بکاپ differential همان ساختار incremental backup را دارد و فقط از فایل های جدید یا فایل هایی که تغییراتی در اطلاعات داشته اند، بکاپ تهیه می کند. بدین ترتیب تمام فایل های ایجاد شده پس از نسخه بکاپ کامل، کپی می شوند. این روش هم به علت جلوگیری از هرگونه بروز مشکل در هنگام تهیه بکاپ، بهتر است به صورت اتوماتیک انجام شود.

٥. Near-CDP Backup

Continuous Data Protection یا محافظت مداوم از داده ها به نسخه بکاپی گفته می شود که بلافاصله پس از ایجاد هر تغییر در اطلاعات، گرفته می شود. این روش اجازه می دهد تا برای بازیابی اطلاعات به هر نقطه ای از زمان که نیاز است مراجعه کرده و از امنیت جامع و پیشرفته ای برخوردار شوید. اپلیکیشن هایی که روش بکاپ Near-CDP را اجرا می کنند معمولا به CDP معروف هستند و به صورت خودکار، نسخه های incremental backup در بازه های زمانی خاص ایجاد می کنند، مثلا هر ۱۵ دقیقه / ۱ ساعت / ۲۴ ساعت. بنابراین برای بازیابی اطلاعات به آن بازه های زمانی مشخص محدود می باشند.

روش Near-CDP backup از ژورنالینگ استفاده کرده و مبتنی بر snapshot ها می باشد و فقط کپی خواندنی از داده های منجمد شده در یک زمان خاص هستند. روش Near-CDP هر تغییری را در سیستم میزبان ثبت می کند، اغلب با صرفه جویی در اختلاف Byte یا Block-level به جای تفاوت در .File-level اختلاف این روش بک آپ با Disk mirroring در این است که امکان بازگشت مجدد Log و در نتیجه بازسازی تصاویر قدیمی داده ها را فراهم می کند.

Intent-logging، اجازه اجرای اقدامات احتیاطی برای سازگاری میانlive data ، محافظت از فایل های self-consistent که نیاز به برنامه های be quiesced and made ready for backup دارند را می هد. روش CDP بکاپ گیری معمولا مناسب برای ماشین های مجازی یا معادل آن است و Near-CDP معمولا برای بکاپ گیری در سرویس Client-server سازمانی استفاده می شود.

بهترین روش‌های پشتیبان‌گیری از اطلاعات

روش‌های مختلفی برای گرفتن بکاپ از اطلاعات وجود دارد که سعی داریم ساده‌ترین و ارزان‌ترین راه‌های بکاپ گیری یا همان پشتیبان‌گیری از اطلاعات را به شما معرفی کنیم. در ادامه به نقاط ضعف و نقاط قوت هر شیوه اشاره خواهیم کرد.

١. کپی کردن اطلاعات روی یک هارد اکسترنال، فلش یا هارد دوم اینترنال به صورت دستی
٢. استفاده از تکنولوژی کلود مثل گوگل درایو یا دراپ باکس
٣. بکاپ گرفتن در بستر اینترنت

و البته اگر از سرورهای تحت شبکه استفاده می‌کنید می‌توانید به صورت دستی یا با استفاده از نرم‌افزارهای خاص به صورت اتوماتیک بروی استوریج‌های مخصوص مثل NAS یا SAN اطلاعات خود را بکاپ گیری کنید.

۱. بک‌آپ گرفتن بر روی هارد اکسترنال یا دستگاه ذخیره‌سازی دیگر

اگر USB یا هارد اکسترنال دارید، به راحتی می‌توانید با استفاده از امکانات خود کامپیوتر، از درایو سیستم بکاپ بگیرید. برای این کار در ویندوز ۱۰ و ۸ می‌توانید از بخش File History استفاده کنید. در ویندوز ۷ از Windows Backup استفاده کنید و در کامپیوترهای مک از Time machine برای بکاپ گیری استفاده کنید. گاهی اوقات می‌توانید هارد را به کامپیوتر نصب کنید و از ابزارهای بک‌آپ‌گیری دیگر استفاده کنید و یا هارد را به سیستم خود متصل نگاه دارید تا خودش به صورت اتوماتیک و طبق برنامه از سیستم شما نسخه پشتیبانی تهیه کند.

- **نقاط مثبت**: بکاپ گرفتن در این روش ارزان و سریع است.
- **نقاط منفی**: اگر منزل شما دچار آتش سوزی شود و یا در آن دزدی رخ دهد، نسخه پشتیبانی شما هم از بین خواهد رفت که فاجعه‌آمیز است.

۲. بکاپ گیری با استفاده از سرویس ذخیره‌ساز ابری

کسانی که در اصول بکاپ گیری خیلی ریزبین هستند، ادعا می‌کنند که استفاده از سرویس ذخیره‌ساز ابری یک روش تکنیکی نیست، اما باید گفت برای اکثر افراد نتیجه مورد هدف را به همراه دارد. به جای آن که فایل خود را بر روی هارد ذخیره کنید، می‌توانید آن را روی سرویس‌هایی مثلDropbox ، Google Drive ، Microsoft OneDrive یا هر سرویس مشابه ذخیره کنید. این سرویس‌ها به صورت اتوماتیک با حساب کاربری شما و کامپیوتر شخصی شما به روزرسانی می‌شوند.

- **نقاط مثبت**: این روش ساده، سریع و در بسیاری از مواقع مجانی است. از آنجایی که اطلاعات شما روی بستر اینترنت است از هر گونه از دست رفتن اطلاعات جلوگیری می‌شود.
- **نقاط منفی**: اکثر سرویس‌های ذخیر سازی ابری فقط چند گیگابایت حافظه را در اختیار کاربران قرار می‌دهند، پس این روش فقط زمانی کاربرد دارد که شما حجم تعداد فایل‌هایی که می‌خواهید بک‌آپ بگیرید کم باشد. مگر این که تمایل داشته باشید برای ارتقای فضای ذخیره‌سازی خود هزینه کنید. بسته به نوع فایل مورد نظر و بک‌آپ آن، این روش می‌تواند ساده‌تر یا پیچیده‌تر از یک کپی ساده بر روی هارد اکسترنال باشد.

۳. بکاپ گرفتن در بستر اینترنت

اگر می‌خواهید مطمئن شوید که فایل‌های شما در امنیت کامل است، می‌توانید از سرویس مثل Backblaze کمک بگیرید و داده‌های خود را در آنجا کپی کنید. Backblaze سرویس آنلاین بک‌آپی است که به خوبی شناخته شده است. در کنار این سرویس‌ها شرکت‌های دیگری مثل Carbonite و MozyHome هم وجود دارند. اگر می‌خواهید مبلغ ماهیانه کمی برای این سرویس‌ها بپردازید مثلا در حدود ۵ دلاردر ماه، آن‌ها انتخاب مناسبی هستند.

این برنامه‌ها در بک‌گراند سیستم شما اجرا می‌شوند و به صورت اتوماتیک داده‌های شما را در سرویس وب خود ذخیره می‌کنند. اگر شما فایل‌ها را از دست بدهید و دوباره به آن‌ها نیاز پیدا کنید به سادگی می‌توانید آن‌ها را بازیابی کنید.

- **نقاط قوت**: بک‌آپ‌گیری آنلاین، شما را در مقابل هر گونه ازدست رفتن اطلاعات یا خرابی درایو، دزدی و فجایع طبیعی و هر چیز دیگری محافظت می‌کند.
- **نقاط منفی**: برای این سرویس‌ها اغلب باید پول بپردازید و در مقایسه با روش بک‌آپ‌گیری در هارد اکسترنال، فرآیند بک‌آپ‌گیری وقت‌گیر است (مخصوصا اگر حجم اطلاعات شما زیاد باشد علاوه‌بر آن از آنجایی که در حال حاضر دلار خیلی گرونه و ما ایرانی‌ها عادت به پرداخت پول برای چنین سرویس‌ها نداریم پس گزینه خوبی نیست.

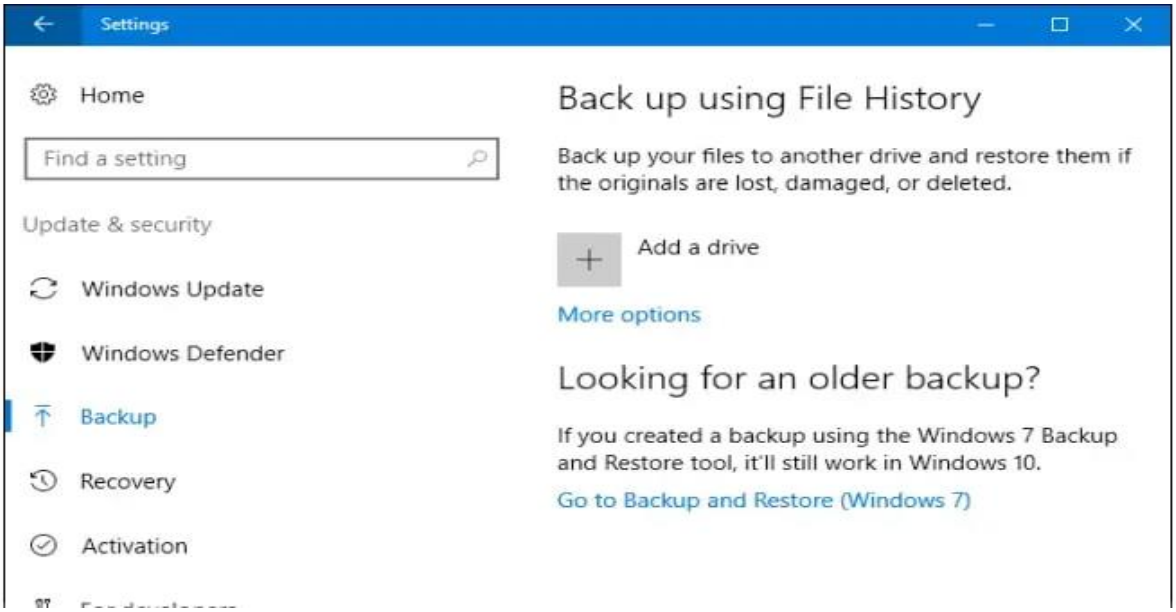
ابزارهای بکاپ گیری در ویندوز

برای آموزش نحوه بکاپ گرفتن از ویندوز ۱۰، انواع روش‌های بکاپ گیری کامپیوتر را بررسی می‌کنیم. ویندوز دارای چند ابزار بکاپ گیری است که برای بک اپ گرفتن از درایو c و دیگر فولدرها و فایل‌ها کاربرد دارد، در ادامه بررسی می‌کنیم.

۱. File History

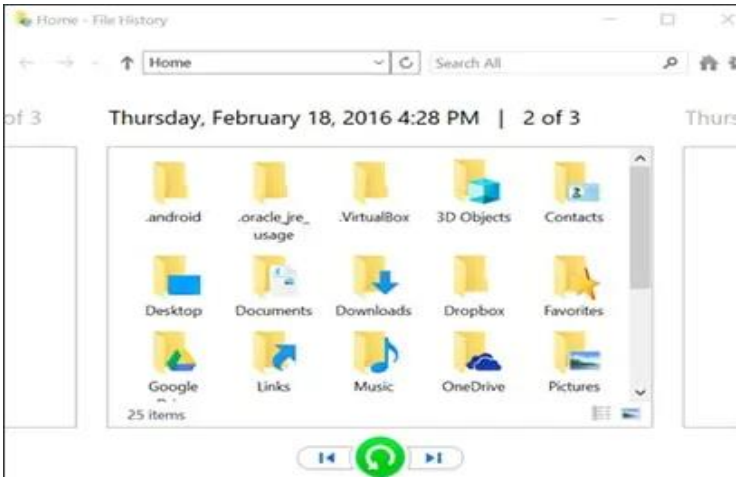
File History برای اولین بار در ویندوز ۸ معرفی شد و هم اکنون جزو راهکارهای بکاپگیری تعبیه شده در ویندوز ۱۰ است. این روش، فول بکاپ از کل پی سی شما ایجاد نمی‌کند اما تمرکز آن روی فایل‌های شخصی شماست تا حتما بکاپ داشته باشند. با تنظیم File History و انجام بکاپگیری مستمر و منظم، و ذخیره بکاپ ها روی هارد اکسترنال همواره مطمئن هستید که نسخه قبلی فایل‌ها را دارید و به راحتی می‌توانید ری استور کنید.

از منوی Setting گزینه Backup را انتخاب کنید.

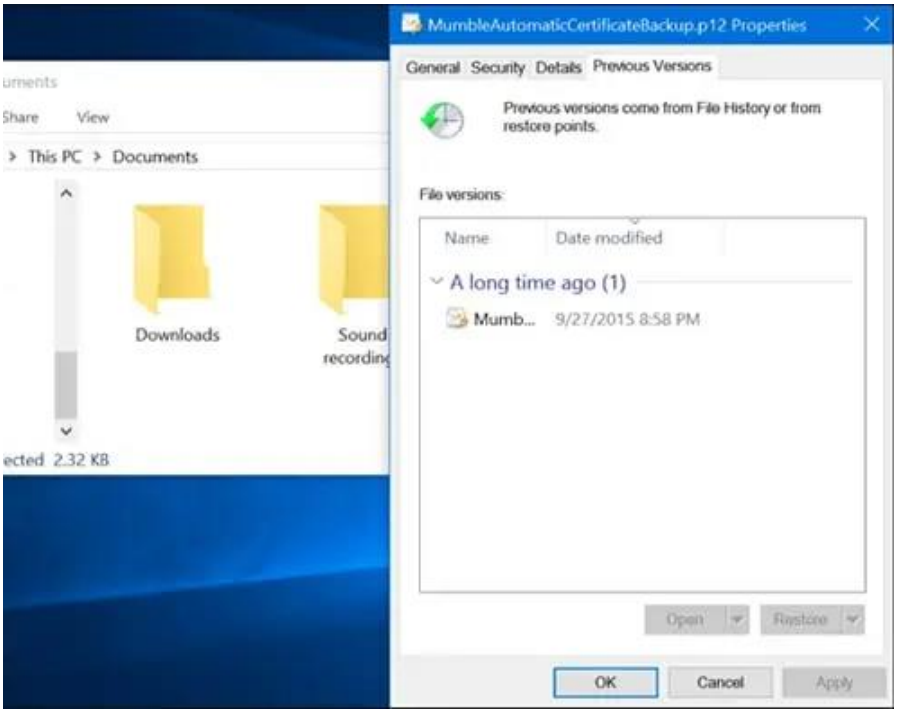


به طور پیش فرض، File Historyاز فولدرهای مهم موجود در فولدر کاربر شما بکاپ می‌گیرد شامل فولدرهای Desktop و Documents و Downloads و Music و Pictures و Videos و AppData می‌توانید فایل‌هایی که نمی‌خواهید بکاپ بگیرید را مشخص کنید.

وقتی نیاز به ریکاوری پیدا کردید می‌توانید مجموعه فایل‌ها و فولدرهای بکاپ گرفته شده را Browse کنید.



یا می‌توانید نسخه‌های قبلی فایل‌ها را از سمت راست و در File Explorer ری استور کنید.



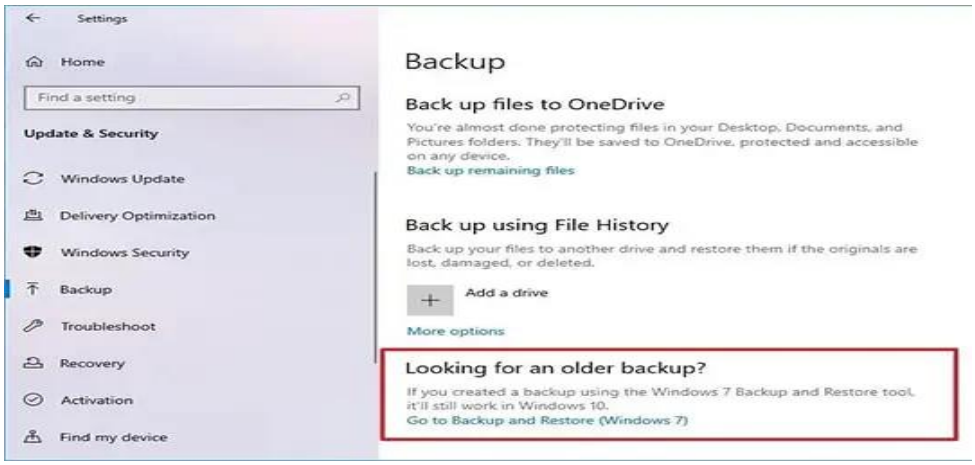
۲. Backup and Restore – Windows ۷

ویژگی Backup and Restore (Windows ۷) tool در ویندوز ۷ و ویندوز ۸ بود از ویندوز ۸.۱ حذف شد اما دوباره در ویندوز ۱۰ وجود دارد. با این قابلیت می‌توانید تمام بکاپ های ویندوز ۷ را به کامپیوتر ویندوز ۱۰ منتقل کنید.

علاوه بر راهکار بکاپ گیری File History که جدیدتر است، می‌توانید از Backup and Restoreاستفاده کنید تا بکاپ هـای هارد دیسک تان را به راحتی ایجاد کنید اما این روش ماننـد File History امکـان نگهـداری نسـخه‌های قـدیمی فایل‌هایتـان را ندارد.

برای تهیه فول بکاپ با استفاده از ابزار سیستمی ویندوز به ترتیب زیر عمل کنید:

۱. از منوی Setting گزینه Backup را انتخاب کنید. سپس از قسمت Looking for an older backup گزینه Go to Backup and Restore -Windows ۷را انتخاب کنید.



به جای این کار می‌توانید مسیر زیر را بروید:

Control Panel > **System and Security** > **File History** > **Backup and Restore (Windows ۷)** > **System Image Backup**

۲. از سمت چپ پنجره گزینه Create a system image را انتخاب کنید.

۳. در این مرحله سیستم به دنبال هارد اکسترنال می‌گردد. حال گزینه On a hard disk را انتخاب کنیـد. حـالا از منـوی دراپ دان می‌توانید درایوهای داخلی یا خارجی را برای ذخیره فول بکاپ خود انتخاب کنید. پس از انتخاب Next بزنید.

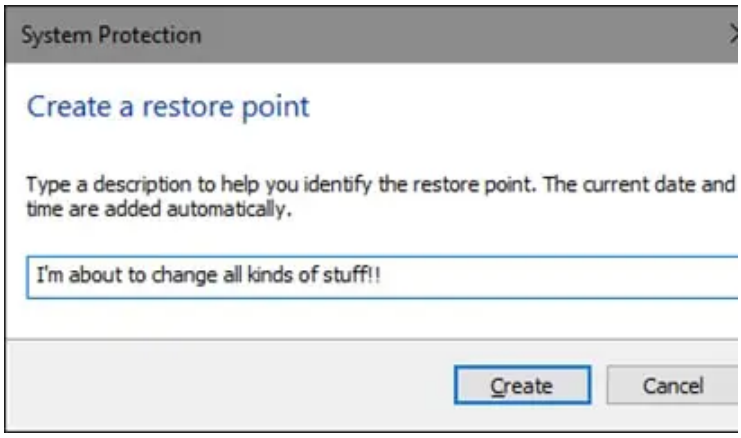
٤. با زدن گزینه Start backup پروسه بکاپگیری آغاز می‌شود.

ابزارهای ریکاوری در ویندوز

۱. System Restore

هنگام بروز مشکل در ویندوز، اگر مشکل با گزینه Fix حل نشود گزینه دیگری با عنوان System Restore در اختیار شما قرار دارد که در واقع نوع خاصی از Fixingاست مثل مواقعی که برنامه تازه نصب شده یا درایور سخت افزاری با مشکل روبرو می‌شود.

System Restore با ایجاد restore points کار می‌کند .اسنپ شات‌هایی از فایل‌های سیستمی ویندوز، فایل‌های برنامه، تنظیمات رجیستری و درایورهای سخت افزاری هستند. هر موقع بخواهید می‌توانید restore point ایجاد کنید اما ویندوز خودش به صورت خودکار هفته‌ای یک بار این کار را می‌کند. همچنین قبل از انجام کار مهم روی سیستم مثل نصب درایور دستگاه جدید با نصب برنامه یا اجرای آپدیت ویندوز، restore point ایجاد می‌کند.



وقتی با مشکلی مواجه شدید می‌توانید System Restore و Restore Point را اجرا کنید تا به آخرین restore point برگردید. با این کار تنظیمات سیستمی، فایل‌ها و درایورها به حالت قبل‌تر خود برمی‌گردند. البته توجه داشته باشید که این قابلیت را در ویندوز خود فعال کنید.

۲. Advanced Startup Options

ویندوز هموار محیط‌هایی را در اختیارتان قرار می‌دهد که بتوانید به عیب یابی مشکلاتی مانند استارت نشدن سیستم بپردازید. در ویندوز ۷ با زدن F۸ هنگام Starting، به advanced startup options دسترسی می‌یابید که گزینه‌های booting into Safe Mode و getting to a Command Prompt را در اختیارتان می‌گذارد.

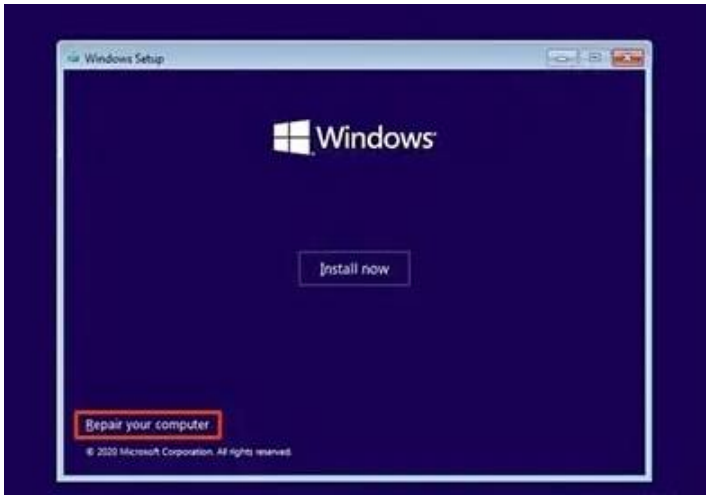
در ویندوز ۸ و ۱۰ قابلیت advanced startup options کمی متفاوت است. اگر ویندوز نتواند به صورت نرمال لود شود، به صورت خودکار advanced options را نمایش می‌دهد. اما راه دسترسی به آن مسیر زیر است:

Settings > Update & security > Recovery > Advanced Startup > click “Restart now.”

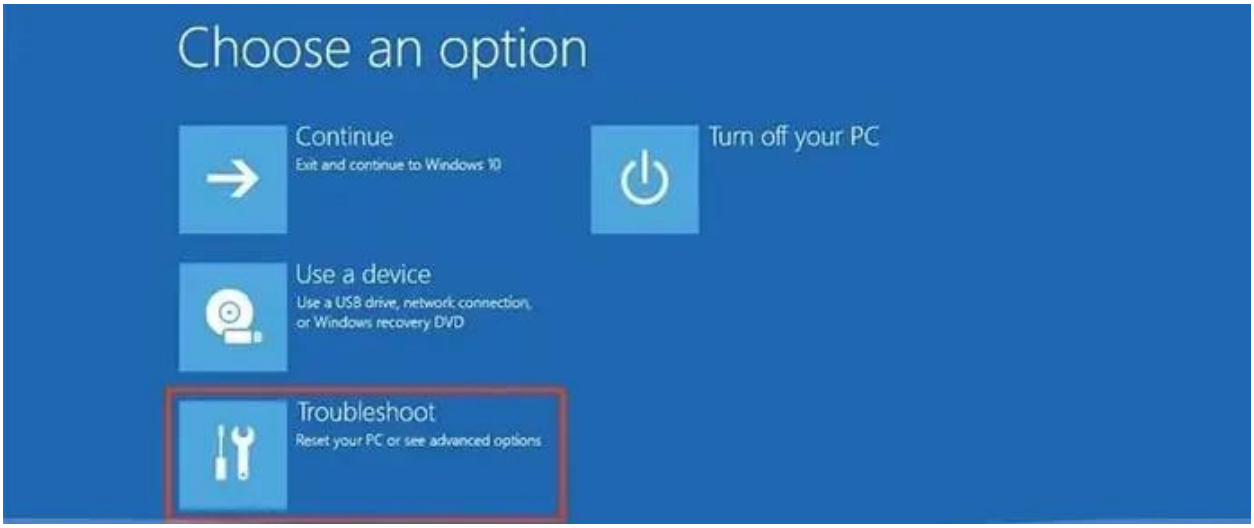
همچنین می‌توانید با زدن دکمه Restart از منوی StartT دکمه Shift را نگه دارید.

نحوه ریکاوری بکاپ ویندوز از طریق DVD و فلش به این شکل است:

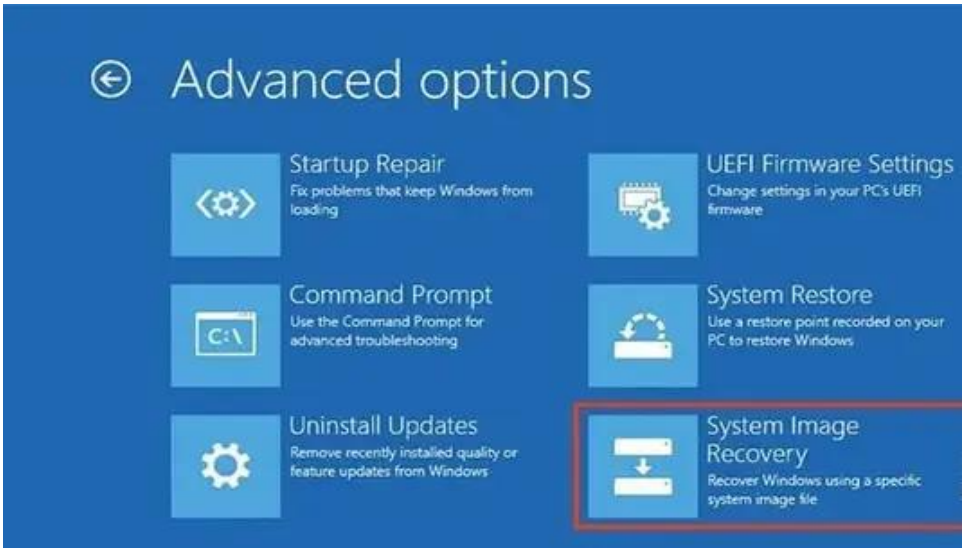
۱. می‌توانید با وارد کردن فلش یا DVD نصب از صفحه نصب، گزینه Repair your computer را از گوشه سمت چپ پایین انتخاب کنید.



۲. گزینه Troubleshoot را بزنید تا پنجره advanced options باز شود.



۳. گزینه System Image Recovery را انتخاب کنید.



٤. ویندوز سرور را از پنجره System Image Recovery انتخاب کنید.

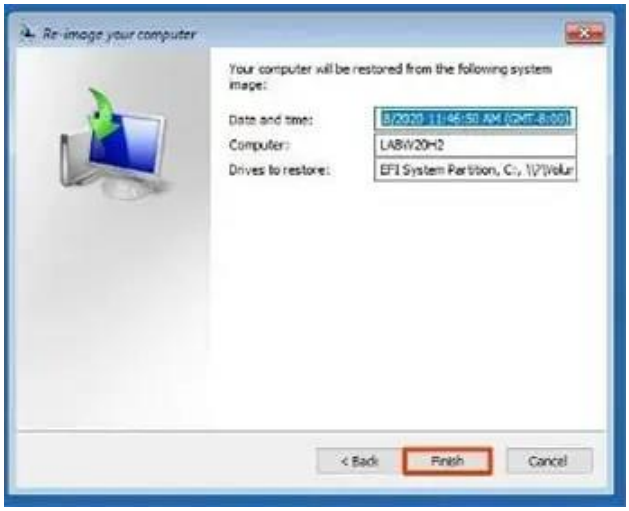
٥. حالا در صفحه Re-image your computer گزینه Use the latest available system image را انتخاب کنید. اگر چندین بکاپ دارید و می‌خواهید به نسخه قدیمی‌تر سیستم و فایل‌ها برگردید، گزینه Select a system imageرا انتخاب کنید Next بزنید.

٦. در این صفحه با دو گزینه روبرو هستید که البته اختیاری است:

١. گزینه Format and repartition disks: اگر می‌خواهید بکاپ را روی درایو جدیدی ری استور کنید، قبل از ری استور کردن بکاپ، گزینه Format and repartition disks را انتخاب کنید. با این انتخاب، گزینه Exclude disksرا استفاده کنید تا از فرمت شدن درایوهای ثانویه که حاوی دیتا هستند جلوگیری شود.

٢. گزینهOnly restore system drivers: اگر بکاپ حاوی کپی چندین درایو است و می‌خواهید فقط سیستم عامل را ری استور کنید، گزینه Only restore system drivers را انتخاب کنید.

۷. حالا به ترتیب Next و Finish و Yes بزنید.



بعد از تکمیل این مراحل، پروسه ریکاوری روی کامپیوتر شروع می‌شود. مدت زمان لازم برای ری استور کردن، بستگی به مقدار دیتا و پیکربندی سخت افزار دارد. در این پروسه وقفه ایجاد نکنید تا ری استورینگ به درستی انجام شود مثلا لپ تاپ را به برق وصل کنید و کامپیوتر را به برقی که دارای UPS است متصل کنید.

۸. حالا با طی مسیر زیر اقدام به نصب آپدیت‌های لازم کنید:

Once the backup has been restored, open **Settings** > **Update & Security** > **Windows Update**> click the **Check for Updates** button

در پنجره advanced options که باز می‌شود می‌توانید ویندوز را از سیستم ایمیجی که ایجاد کردید، ری استور کنید. گزینه System Restoreبرای رفع مشکل و انجام تسک هایی در زمینه maintenance است. اگر در حال اجرای preview

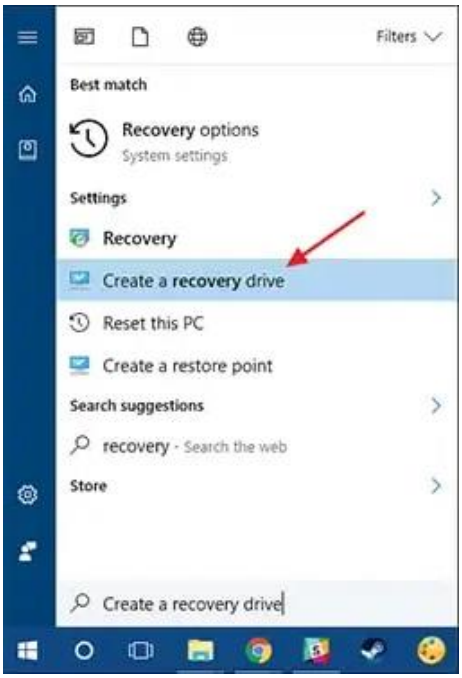
builds of Windowsهستید و بیلد جاری درست کار نمی‌کند یا لود نمی‌شود، با این منو می‌توانید به بیلد قبلی برگردید. این منو وقتی ویندوز به صورت نرمال لود نمی‌شود هم نمایش داده می‌شود.

۳. Recovery Drive Creator

در ویندوز امکان ایجاد درایو ریکاوری برای شما وجود دارد که حتی اگر نصب ویندوز به کل از بین برود و به منوی Advanced Startup Optionsدسترسی نداشته باشید، می‌توانید هارد درایوی را جایگزین کنید و image backup را ری استور کنید.

نحوه ایجاد درایو ریکاوری بدین شکل است:

۱. در قسمت سرچ ویندوز Recovery را تایپ کنید و گزینه Create a recovery drive را انتخاب کنید.



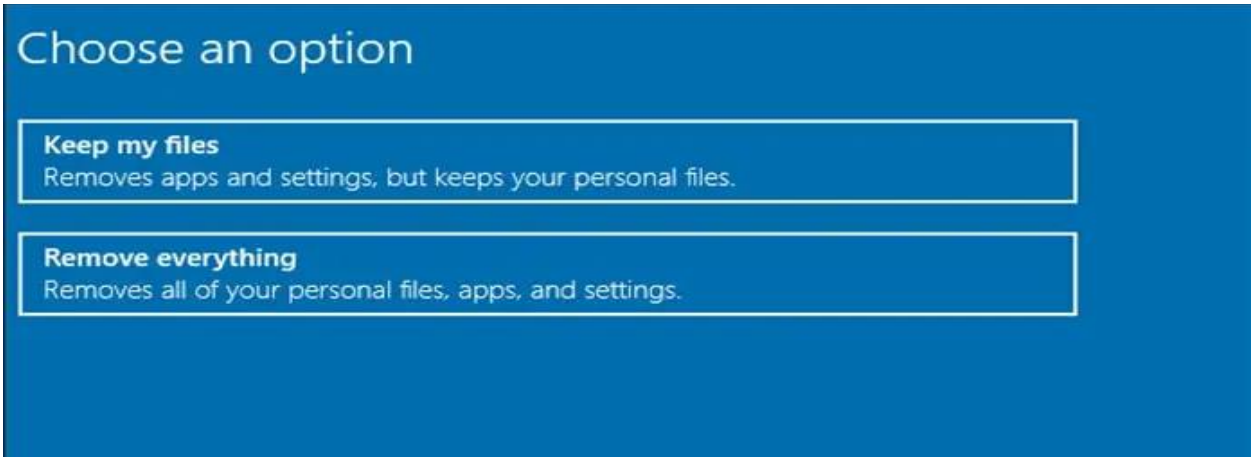
۲. تنها کاری که شما در ویزارد Recovery Drive باید انجام دهید این است که درایو را انتخاب کنید: در ویندوز ۷ باید CD/DVD و در ویندوز ۸ و ۱۰ باید USB انتخاب کنید. در ادامه کار کپی انجام می‌شود.

۳. پس از پایان کار، درایو خود را برچسب بزنید و جای امنی قرار دهید تا وقتی ویندوزتان نتواست لود شود از آن استفاده کنید.

۴. Reset This PC

ویژگی Reset this PC یکی از قابلیت‌های خوبی است که به ویندوز ۸ و ۱۰ اضافه شد که برای ری استوری کردن کامپیوتر به وضعیت پیش فرض سیستم عامل به کار می‌رود Reset this PC .جایگزین نصب مجدد ویندوز با USB و DVD است. با این گزینه به جای نصب مجدد به ویندوز می‌گویید و ویندوز آن را برایتان انجام می‌دهد. همچنین می‌تواند فایل‌های شخصی شما را سر جایشان نگه دارند.

آموزش نصب ویندوز ۱۰



در ویندوز ۸ گزینه‌های Refresh your PC و Reset your PC جدا هستند. اولی تنظیمات و فایل‌های شخصی شما را نگه می‌دارد اما تنظیمات PC را به حالت پیش فرض برده و برنامه‌های دسکتاپی شما را uninstall می‌کند. دومی همه چیز را پاک می‌کند حتی فایل‌هایتان را، انگار که دوباره ویندوز نصب می‌کنید. در ویندوز ۱۰ گزینه ریست به شما دو گزینه می‌دهد: فایل‌های شخصی شما هنگام پروسه ریست، پاک شوند یا نگه داشته شوند.

اگر همه چیز را پاک کنید، می‌توانید به ویندوز بگویید که securely erase the drive را انجام دهد. این امکان برای وقتی خوب است که می‌خواهید کامپیوتر و لپ تاپ خود را بفروشید.

ریکاوری داده

ریکاوری داده فرایند بازیابی داده‌ای است که به صورت اتفاقی یا از قصد از دست رفته است. در محیط سازمانی، این مساله شامل داده‌هایی که امکان دسترسی به آن‌ها از بین رفته است نیز می‌شود. با این که در برخی موارد می‌توانید خودتان در چندین جای مختلف مثل سطل زباله‌ی سیستم عامل دنبال اسناد مورد نظرتان بگردید، در بیشتر موارد به یک ابزار نیاز خواهید داشت که این کار را برای شما انجام دهد.

مزیت واضح استفاده از یک ابزار برای ریکاوری داده این است که این ابزارها سریع‌تر هستند، جستجوی کامل‌تری انجام می‌دهند و می‌توانند داده را از جاهایی که دسترسی به آن‌ها امکان‌پذیر نیست، یا حتی بعضی اوقات مکان‌هایی که حذف شده‌اند، بازیابی کنند. تنها پیش‌نیاز کارکردن آن‌ها این است که درایو باید از نظر فیزیکی سالم بوده و به‌درستی کار کند. همین! بقیه‌ی مراحل را این ابزارها برای شما انجام می‌دهند.

نحوه انتخاب یک ابزار ریکاوری داده

با توجه به این که گزینه‌های فراوانی پیش رو دارید، انتخاب چندان راحت نیست. در اینجا چند ویژگی مختلف را که می‌توانید هنگام انتخاب یک ابزار ریکاوری داده در نظر بگیرید آورده‌ایم.

۱. امکانات

یکی از مهم‌ترین ملاحظات هنگام انتخاب ابزار ریکاوری داده مجموعه امکانات آن است. یک ابزار چه امکاناتی را در اختیار شما قرار می‌دهد، و آیا این امکانات می‌توانند مشکل شما را حل کنند؟ اگر جواب بله است، آن ابزار را انتخاب کنید. اگرنه، دنبال دیگر گزینه‌ها باشید.

قبل از تصمیم‌گیری درباره امکانات، لیستی از قابلیت‌هایی که دوست دارید یک ابزار ریکاوری داده داشته باشد تهیه کنید. این احتمالا یک نقطه‌ی خوب برای شروع است چون همه‌ی کاری که لازم است انجام دهید این است که لیست خود را با قابلیت‌های هر ابزار مقایسه کنید. وقتی یک مورد با مطابقت زیاد پیدا کردید، به آن معناست که ابزار ایده‌آل خود را یافته‌اید.

۲. شرکت عرضه‌کننده‌ی ابزار

پشت هر ابزاری یک شرکت هست که آن را ارائه کرده و اطمینان از این که این شرکت قابل اعتماد و باتجربه باشد اهمیت بالایی دارد. حتما بررسی‌های آنلاین ابزارها را مطالعه کنید.

اعتبار شرکت ارائه‌دهنده‌ی ابزار اهمیت فراوانی دارد چون شرکت‌های کلاهبردار معمولا از ابزارهای خود به عنوان راهی برای سرقت اطلاعات ارزشمند از کامپیوتر شما استفاده می‌کنند. به عبارت دیگر، برخی ابزارها مخرب بوده و شما باید از آن‌ها پرهیز کنید. بررسی سابقه‌ی فروشنده‌ی نرم‌افزار نیز اهمیت فراوانی دارد.

۳. گزینه‌های مختلف برای پیش‌نمایش و فرمت‌های متنوع

ابزار ریکاوری که انتخاب می‌کنید باید امکان پیش‌نمایش فایل‌های آسیب‌دیده را داشته باشد تا بتوانید مطمئن شوید فایل درستی را ریکاوری می‌کنید. این کار باعث صرفه‌جویی به‌شدت زیادی در زمان و زحمت لازم برای ریکاوری فایل‌ها می‌شود. علاوه بر این، ابزار انتخاب‌شده باید از فرمت‌های مختلف فایل‌ها پشتیبانی کند، تا نه‌تنها بتوانید اسناد را بازیابی کنید، بلکه بتوانید فایل‌های صوتی، ویدئویی و حتی تصاویر را هم ریکاوری کنید. به علاوه، ابزار انتخابی باید توانایی بازیابی اسناد از هرگونه بستر، فضای ذخیره‌سازی یا دستگاه الکترونیکی را داشته باشد تا بالاترین سطح انعطاف‌پذیری را برای شما فراهم کند.

٤. سیستم مورد نیاز

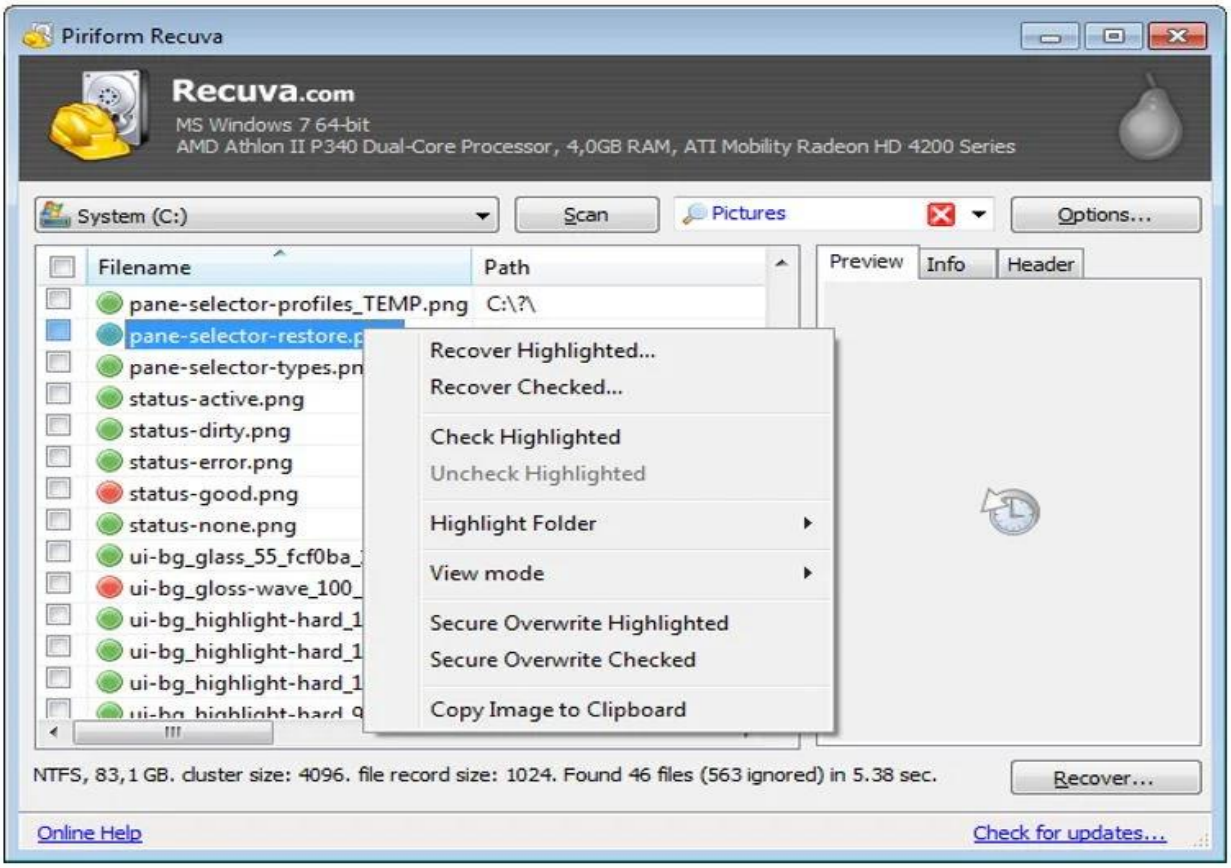
سیستم مورد نیاز برای نرم‌افزار را بررسی کرده و اطمینان حاصل کنید سیستم شما مناسب اجرای آن باشد. با این کار تضمین می‌کنید ابزار از تمام قدرت و قابلیت‌های خود بهره بگیرد. در غیر این صورت ممکن است تجربه‌ی کاربری ناخوشایندی از استفاده از ابزار داشته باشید یا حتی بدتر از آن، ممکن است ابزار به کلی روی سیستم شما کار نکند.

٥. هزینه

هزینه نیز یکی دیگر از ملاحظاتی است که باید در نظر داشته باشید. امروزه ابزارهای رایگان زیادی در دسترس هستند و در همین پست هم لیست بلندی از ابزارهای رایگان ریکاوری اطلاعات هستند که در ادامه آن‌ها را خواهید دید. با وجود این که این ابزارها می‌توانند کار شما را راه بیندازند، می‌توانید سراغ گزینه‌های پولی هم بروید، به خصوص اگر دنبال یک قابلیت خیلی خاص باشید. به علاوه ابزارهای پولی معمولا توسط کمپانی‌های معروف ارائه می‌شوند، به همین خاطر خیالتان از ایمنی و امنیت آن‌ها راحت است.

آشنایی با یک نرم افزار ریکاوری فایل (Rucuva)

در دو نسخه‌ی رایگان و پولی ارائه شده و ابزاری فوق‌العاده قدرتمند برای ریکاوری داده از پارتیشن‌های لینوکسی و ویندوزی است. این ابزار با پشتیبانی از تمام نسخه‌های ویندوز از XP گرفته تا ۸.۱، ابزاری فوق‌العاده برای بازیابی داده‌های ازدست‌رفته است. کارایی این ابزار در طول سالیان متمادی در عمل ثابت شده است.



امکانات :

- **امکان تنظیم بازنویسی فضای خالی به صورت ایمن در ویندوز ۱۰**
- **تشخیص درایوها و پارتیشن‌ها**
- **بازیابی فایل‌های با قالب‌های پراستفاده**
- **مجهز به حالت اسکن عمیق پیشرفته برای یافتن هرگونه نشانه از فایل ازدست‌رفته**

۵ اشتباه رایج هنگام تهیه نسخه بکاپ

تا به اینجا در خصوص مسائل مربوط به اهمیت تهیه نسخه پشتیبان و مزیت های آن صحبت شده است. در ادامه به برخی توصیه ها و همچنین اشتباهات رایجی که در طول تهیه نسخه بکاپ متداول است خواهیم پرداخت.

۱. **عدم نیاز به پشتیبان گیری از برخی اطلاعات**

بدون شک این یکی از رایج ترین اشتباهات است. خیلی اوقات تهیه نسخه بکاپ یا به دلیل عدم دسترسی به اطلاعات یا بـه دلیـل اینکه اطلاعات در آن زمان مهم نبوده است انجام نشده، تا زمانی که از بین بروند.

۲. **ذخیره نسخه های پشتیبان در همان سخت افزاری که فایل اصلی می باشد**

دلیل تهیه نسخه بکاپ از اطلاعات برای نگهداری از آنها می باشد. بنابراین کپی داده ها باید در مکـانی متفـاوت از محـل نگهـداری اطلاعات اصلی ذخیره شود. اگر آنها در همان سخت افزار ذخیره شده و سخت افزار آسیب ببیند، نسخه های بک آپ نیز همـراه بـا اطلاعات اصلی از بین خواهند رفت.

۳. **تست نسخه بکاپ**

تهیه نسخه بکاپ شامل فرآیند های مختلفی می باشد. فقط ایجاد یک نسخه کافی نیست، همچنین پس از تهیـه نسـخه پشـتیبان باید اطلاعات را بررسی کنید تا در صورت نیاز به داده های ذخیره شده واقعاً در دسترس باشند. آزمایش نسخه بکاپ تهیه شـده بـه همان اندازه فایل اصلی دارای اهمیت است. بسته به نوع بکاپ تهیه شده، که اغلب به صورت فایل فشرده شده اسـت، ممکـن اسـت در زمان تست خراب شود، در این صورت باید یک نسخه پشتیبان تهیه کرد.

٤. **به طور منظم و به اندازه کافی نسخه پشتیبان تهیه نمی شود**

تهیه نسخه پشتیبان به طور منظم بسیار مهم است، خصوصاً اگر اطلاعات به طور مکرر به روز می شوند. به عنوان مثال تصور کنیـد در حال نوشتن کتاب هستید، در یک نرم افزار مرتبط برای نوشتن هستید و فقط در اول هر ماه یک نسخه پشتیبان تهیه می کنید. اگر فایل در میان ماه دچار مشکل شود، شما تنها یک نسخه که مربوط به ۲ هفته قبل است را خواهید داشت و تمام کارهایی را که در این دوره انجام داده اید از دست خواهید داد.

٥. **عدم برچسب زدن به فایل های بکاپ**

پس از اجرای نسخه پشتیبان، فایل های تهیه شده از هر آرشیو و مربوط به هر سخت افزار را نگهـداری کنیـد. در صـورت نیـاز بـه ریکاوری اطلاعات برای تجهیزات مختلف، این کار به صورت درست برای تجهیزات درست انجام خواهد شد.

منابع:

https://falnic.com/blog/glossary-what-is-data-protection-or-data-protection.html

https://liangroup.net/blog/gfi-top-۲۳-recovery-tools-۲۰۲۰/

https://www.keysun-co.com/data/