نیاز به قواعد اکتشافی

P.T. Davis

متخصصان اطلاعات و امنیت سایبری در جهان امروز، به مجموعه خوبی از قواعد اکتشافی نیاز دارند، گرچه همیشه برای تحلیل کامل تصمیم یا ارزیابی ریسک، هیچ داده یا توانایی تمام و کمالی وجود ندارد. بنابراین، گاهی اوقات به‌قول **هربرت ســـیمون** (Herbert A. Simon) باید *"به رضایت تـــن دهید."* از اینرو، برای دســـتیابی به پاســـخی قانع‌کننده به یک «قاعده کلی»، میانبر ذهنی، راهبرد ذهنی ساده یا روشهای بهتر نیاز دارید.

گاهی اوقات شما توانایی بررسی مسائل را به‌صورت رسمی، عقلانی، منظم، خطی، منطقی و با تأمل دارید؛ اما در زمانهای دیگری که این توانایی را نداشته باشید، مسائل را به‌طور غیررسمی، غیرعقلانی، مستقیم، غیرخطی، غیرمنطقی و احساسی بررسی خواهید کرد. در چنین شرایطی، باید قواعد اکتشافی را برای وضعیت دوم اســـتفاده کنید. این قواعد در عین‌حال بخشـــی از سامانه پردازش تجربی سازگار و

بزرگتر هستند.

یک الگو، ممکن اســت نمونه خوبی از یک قاعده اکتشــافی باشد؛ گرچه دنیای واقعی هرگز مانند الگو نیســت، اما به شما کمک خواهد کرد تا دنیای واقعی را درک کنید.

ارزیابی ریســک مثال خوبی برای الگوسازی اســت. می‌توانید ریسک را الگوسازی کنید، اما قابل پیش‌بینی نیســت. من به‌هنگام ارائه مشاوره، از قاعده اکتشافی استفاده می‌کنم؛ زیرا نوشــتن گزارش دو برابر بیشتر از انجام کار آن طول می‌کشد. شاید تاکنون کاشف قانون هفت یا قانون کاشف نصف سن‌تان به‌اضافه هفت به گوشتان خورده باشد. از این نمونه قواعد اکتشافی در همه جا هستند.

قواعد اکتشــافی زیادی در کسب‌وکار اســتفاده می‌شوند. اما متأســفانه برخی از آنها جانبدارانه هســتند؛ به‌ویژه هنگامی که با مدیریت ریسک ســروکار داریم. برای مثال، هنگامــی که مردم در مورد احتمال وقوع رویدادی به‌آســانی قضــاوت می‌کنند، **قواعد اکتشافی در دسترس**[1] پدید می‌آید.

به‌عنوان نمونه‌ای دیگر؛ اگر از شــما بپرسم فیلها ممکن است انسان را بیشتر بکشند یا کوســه‌ها، کدامیک را نام می‌برید؟ بیشــتر مــردم با توجه به اخبــار روزنامه‌ها، اخبار تلویزیونی و دیگر اطلاعات، به طرز شــگفت‌آوری مورد کوسه را جواب می‌دهند. با این حال، احتمال کشــته شدن انسان به‌وســیله فیل ده برابر بیشتر از احتمال کشته شدن او به‌وسیله کوسه است (همچنین، اگر فقط آمار حمله سگها به انسان را بررسی کنید و حتی مرگ‌ومیر ناشــی از هاری را هم در نظر نگیرید، آنها دســتکم ۳ برابر بیشتر از کوسه‌ها شما را می‌کشند.)

از ســوی دیگر، برخی قواعد اکتشافی مفیدند. یکی از قواعد اکتشافی که می‌توانید از آن به‌طور منطقی در ارزیابی ریسک استفاده کنید، **قواعد اکتشافی مشابهت**[2] است و آن در جایی است که می‌توانید براساس شباهت بین وضعیت فعلی خود و دیگر وضعیتها یا الگوهای آن وضعیتها، قضاوت کنید.

در ارزیابی ریســک، همیشــه نمی‌توانید به داده‌های موردنیاز خود دسترسی داشته باشید؛ اما می‌توانید در زمینه‌ها، رشــته‌ها یا حرفه‌های دیگر، موقعیتهای مشابهی پیدا کنید که بتوانند به‌عنوان نمونه عمل کنند.

موارد زیــر به‌عنوان قاعده‌ای اکتشــافی در زمینه اطلاعات و امنیت ســایبری، ارائه می‌شود:

- **دفاع عمیق**: کنترلها بدون خطا نیســتند؛ بنابراین نبایــد روی یکی از آنها، بلکه باید روی چند کنترل تکیه کنید.
- **دوبارگــی**: مؤلفه‌های کلیدی نیاز به پشــتیبان‌گیری دارند. اگر مؤلفه مهمی وجود دارد، ممکن اســت بخواهید آن را با یک مؤلفه اضافی پشــتیبان‌گیری کنید. به فکر پردازنده باشید و هر کاری برای دسترســی به سامانه موردنیازتان لازم است، انجام دهید. این کار با قاعده اکتشــافی «به‌قدری مهم است که نباید شکست بخورد»، و با

یک الگو ممکن است نمونه خوبی از یک قاعده اکتشافی باشد گرچه دنیای واقعی هرگز مانند یک الگو نیست اما به شما کمک خواهد کرد تا دنیای واقعی را درک کنید

قانون مورفی (Murphy's Law)، در یک راستاست.

- **منحنی بل**: هنگامی که ۵ کارمند یا بیشتر دارید، ۱۰ درصد شرکت را ترک می‌کنند تا رقیب شما شوند.
- **خرابی سامانه**: سامانه‌ها در بدترین زمان ممکن، یعنی پایان عمر یا پایان سال خراب می‌شوند.
- **ترس، نبود اطمینان و تردید**: مردم به ترس، نبود اطمینان و تردید، واکنش نشان می‌دهند. این نمونه‌ای از **قواعد اکتشافی عاطفی**[3] است که در آن، مردم به احساسات فعلی خود اجازه می‌دهند تا بر تصمیمهایشان تأثیر بگذارند و مشکلاتشان را به‌سرعت و به‌طور مؤثر حل کنند. هنگامی که مشکلی پیچیده و غیرخطی دارید و با احساس غریزی خود آن را حل می‌کنید، این یک کار مثبت است.
- **رمز عبور**: اگر بیشتر از ۲۳ کارمند دارید، ۵۰ درصد احتمال وجود دارد که رمز عبور یکی از آنها ضعیف باشد.
- **امنیت ۸۰/۲۰**: باید ۸۰ درصد زمان خود را برای برنامه‌ریزی و ۲۰ درصد را در هنگام اجرا صرف کنید.
- **مبتنی‌بر قانون**: اگر راهکارتان برای مبارزه با ویروسهای رایانه‌ای فقط براساس قانون باشد، بدافزار وارد سامانه‌تان می‌شود.
- **آزمون کامپیوتر خدمت‌رسان**: آزمون کامپیوتر خدمت‌رسان که روی اینترنت است، حلقه ضعیف یا پاشنه آشیل و دروازه‌ای به شبکه شماست.
- **رمزگذاری**: تونلی بر پایه **شبکه گسترده جهانی** (WAN) بسازید و به **شبکه محلی** (LAN) انتقال دهید.

ما نیز باید همچون متخصصان اطلاعات و امنیت سایبری، برای ایجاد مجموعه مفیدی از قواعد اکتشافی تلاش کنیم. هنگامی که این قواعد به‌طور صحیح استفاده شوند، در زمان تصمیم‌گیری‌های سریع توانمند خواهیم بود. اما اطمینان حاصل کنید که این قواعد برای دلایل مناسب به کار می‌روند و اینکه جانبداری منفی در کارتان ندارند.

ما نیز باید همچون متخصصان اطلاعات و امنیت سایبری برای ایجاد مجموعه مفیدی از قواعد اکتشافی تلاش کنیم هنگامی که این قواعد به‌طور صحیح استفاده شوند در زمان تصمیم‌گیری‌های سریع توانمند خواهیم بود

پانوشتها:

1- Availability Heuristic
2- Similarity Heuristic
3- Affect Heuristic

منبع:

Davis P.T., **The Need for Heuristics**, www.isaca.org, 2016