INVESTECH
Invest in Tech

فصلنامه خبری تحلیلی

اینوستک

آشنایی با تامین مالی جمعی و بررسی تازه‌ترین آمار این حوزه، آشنایی با امنیت سایبری و تازه‌ترین آمارهای آن

پاییز ۱۴۰۲

شرکت اینوستک در سال ۱۴۰۰ با هدف سرمایه‌گذاری بلندمدت در زمینه فناوری اطلاعات و امنیت سایبری و با برند تجاری INVESTECH کار خود را آغاز کرد. اینوستک، در بدو تأسیس با ورود به ۴ استارتاپ باسابقه و دارای پتانسیل رشد، سعی به افزایش توانمندی خود در این زمینه را داشته است. این شرکت با تملک سهام شرکت‌های دارای قابلیت بالا در زمینه ICT توانسته است در رشد فناوری و زمینه‌سازی امنیت زیرساخت و سایبری، نقش مثبتی ایفا کند که یکی از این موارد، مشارکت در ایجاد صندوق پژوهش و فناوری فن‌آسا می‌باشد.

اینوستِک

سرمایه‌گذار و سرمایه‌پذیر هوشمند

فهرســـت محتـــوا

استراتژیست محتوا وطراحی : ناهید سادات ریاحی (دانشجوی دکترای شیمی-فیزیک در دانشگاه شهید بهشتی)
هیئت مشاوره: دکتر محمدصادق علیزاده (مدیرعامل اینوستک و دکترای برق از دانشگاه صنعتی شریف)
دکتر علیرضا نواب‌پور (مدیرعامل صندوق فن‌آسا و دکترای مدیریت مالی از دانشگاه امام صادق)
دکتر زهرا سهرابی (معاونت امور راهبردی و دکترای برق از دانشگاه صنعتی شریف)
دکتر حبیب‌اله یاجم (مشاور کارگروه علمی و دکترای برق از دانشگاه تهران)

تامین مالی جمعی چیست؟

تامین مالی جمعی (crowdfunding) روشی برای تامین مالی است که شامل ایجاد یک کمپین در یک بستر آنلاین و درخواست از مردم برای کمک مالی در ازای سود یا حقوق صاحبان سهام است. تامین مالی جمعی می‌تواند به کسب‌وکارها کمک کند تا ایده خود را آزمایش کرده، بازخورد کسب نموده، پایگاه مشتری ساخته و سرمایه‌گذاران بیشتری را جذب کنند.

تصور کنید که بتوانید چیزی شگفت‌انگیز خلق کنید، آن را با جهان به اشتراک بگذارید و توسط هزاران نفر حمایت شوید که به شما و دیدگاه شما اعتقاد دارند. این معنای تامین مالی جمعی است؛ روشی انقلابی برای تامین مالی ایده، پروژه یا هدف تجاری کسب‌وکارها با جمع‌آوری پول به صورت آنلاین از تعداد زیادی از افراد. در این روش، تعداد زیادی از شهروندان بر روی یک استارت‌آپ یا طرح سرمایه‌گذاری می‌کنند. این سرمایه‌گذاری معمولاً از طریق اینترنت و با استفاده از سکوهای تأمین مالی جمعی صورت می‌پذیرد. یک بنیان‌گذار به جای آن که به دنبال سرمایه‌گذاران و شرکت‌های

سرمایه‌گذاری برود، طرح و ایده خود را در پلتفرم‌های تأمین مالی ارائه می‌کند و سرمایه‌گذاران با دیدن این طرح‌ها می‌توانند با کمترین سرمایه ممکن، در این طرح‌ها مشارکت کرده و در سود و زیان آن نیز شریک شوند. بنابراین تامین مالی جمعی یک روش نوآورانه برای جمع‌آوری پول برای پروژه‌ها، اهداف و مشاغل مختلف با استفاده از قدرت جمعی جمعیت است. با توجه به وجود برخی چالش‌ها، اجرای یک برنامه تامین مالی جمعی، به برنامه‌ریزی، اجرا و ارتباطات دقیق برای اطمینان از موفقیت نیاز دارد. تامین مالی جمعی نه تنها راهی برای تامین مالی، بلکه راهی برای خلق، اشتراک گذاری و ارتباط است. آمارها نشان می‌دهند که تامین مالی جمعی یک روش محبوب و موثر برای جمع آوری پول برای اهداف مختلف است و پتانسیل بسیار زیادی برای رشد و تاثیر دارد.

مزایا و چالش‌ها

مزایای تامین مالی جمعی عبارتند از: اعتبار بخشیدن به ایده‌ها با دریافت بازخورد و حمایت از مشتریان و سرمایه‌گذاران بالقوه، جمع‌آوری سریع و آسان سرمایه بدون نیاز به سهام یا سرمایه‌گذاران سنتی، ایجاد جامعه‌ای وفادار از حامیان که می‌توانند اطلاعات مربوط به محصولات یا خدمات را منتشر کرده و بینش‌ها و پیشنهادات ارزشمندی را ارائه دهند.

از جمله چالش‌های تامین مالی جمعی، خصلت رقابتی بالاست، زیرا استارت‌آپ‌ها باید یک کمپین جذاب ایجاد کنند، پاداش‌های جذابی ارائه دهند و به طور موثر با حامیان خود ارتباط برقرار کنند. خطراتی مانند سرقت مالکیت معنوی یا عدم تحقق وعده‌ها، تأثیرات منفی بر شهرت و اعتبار استارت‌آپ‌ها در صورت برآورده نکردن انتظارات حامیان، از دیگر چالش‌های این روش هستند.

انواع تامین مالی جمعی

مبتنی برخیریه: این نوع تأمین مالی جمعی برای جمع‌آوری پول برای یک هدف، یک خیریه یا یک نیاز شخصی، بدون انتظار هیچ‌گونه بازگشتی از سوی مشارکت کنندگان، استفاده می‌شود. مردم به این دلیل پول اهدا می‌کنند که به هدف اعتقاد دارند یا می‌خواهند به فردی نیازمند کمک کنند. برخی از نمونه‌های پلتفرم‌های تامین مالی جمعی مبتنی بر خیریه عبارتند از: GoFundMe، JustGiving و GiveIndia. این روش در ایران نیز توسط ارگان‌ها و افراد مختلفی در زمان بحران‌هایی همچون زلزله انجام می‌شود.

مبتنی بر پاداش: این نوع تامین مالی جمعی برای جمع‌آوری پول برای محصول یا خدماتی که هنوز در بازار موجود نیست، از طریق ارائه پاداش به مشارکت کنندگان بر اساس مبلغی که اهدا می کنند، استفاده می‌شود. جوایز می‌تواند هر چیزی باشد، از یادداشت تشکر گرفته تا نمونه رایگان محصول یا خدمات. برخی از نمونه‌پلتفرم‌های سرمایه‌گذاری جمعی مبتنی بر پاداش عبارتند از Kickstarter، Indiegogo و Patreon. در ایران نیز

استارت‌آپ نیک استارتر تجربه این نوع تامین مالی جمعی را دارد اما گسترش زیادی نیافته است.

مبتنی بر سهام: این نوع تامین مالی جمعی برای جمع‌آوری پول برای یک استارت‌آپ یا کسب‌وکار از طریق ارائه سهام به مشارکت‌کنندگان، که به سرمایه‌گذاران شرکت تبدیل می‌گردند، استفاده می‌شود. سرمایه گذاران می‌توانند از رشد و موفقیت شرکت بهره‌مند شوند، اما خطر شکست را نیز می‌پذیرند. برخی از نمونه‌پلتفرم‌های تامین مالی جمعی مبتنی بر سهام عبارتند از Seedrs، Crowdcube و Wefunder.

مبتنی بر بدهی: این نوع تأمین مالی به صورت وام صورت می‌پذیرد که در آن متقاضی متعهد می‌شود تا پس از مدت محدودی، پول سرمایه‌گذاران را به همراه بهره قطعی به آن‌ها برگرداند.

داستان‌های موفق تامین مالی جمعی

Oculus: یک شرکت واقعیت مجازی است که Oculus Rift را ایجاد کرده است، هدستی که به کاربران اجازه می‌دهد محیط‌های سه‌بعدی فراگیر را تجربه کنند. این شرکت در سال ۲۰۱۲ کمپین Kickstarter را برای جمع‌آوری ۲۵۰ هزار دلار راه‌اندازی کرد، اما تنها در عرض چهار ساعت از هدف خود فراتر رفت و در مجموع ۲٫۴ میلیون دلار از بیش از ۹۵۰۰ حامی جمع‌آوری کرد. این کمپین سر و صدای زیادی ایجاد کرده و توجه فیس‌بوک را به خود جلب نمود، به طوری که Oculus را با قیمت ۲ میلیارد دلار در سال ۲۰۱۴ خریداری کرد. Oculus اکنون یکی از بازیگران پیشرو در صنعت VR است که میلیون ها کاربر و توسعه‌دهنده در سراسر جهان دارد.

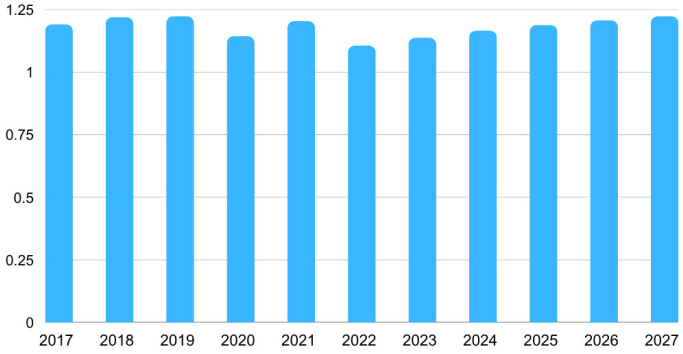
Pebble: یک شرکت ساعت هوشمند است که پیشگام بازار فناوری پوشیدنی است. این شرکت اولین کمپین Kickstarter خود را در سال ۲۰۱۲ برای جمع آوری ۱۰۰ هزار دلار برای ساعت الکترونیکی Pebble E-Paper راه‌اندازی کرد، اما مبلغ هدف اولیه خود را رد کرده و بیش از ۱۰ میلیون دلار از بیش از ۶۸ هزار حامی جمع‌آوری کرد. این کمپین به قدری موفقیت‌آمیز بود که در آن زمان به بیشتر ین سرمایه در

Kickstarter تبدیل شد. Pebble دو کمپین تامین مالی جمعی دیگر را در سال‌های ۲۰۱۵ و ۲۰۱۶ برای ساعت‌های Pebble Time و Pebble ۲ راه‌اندازی کرد که به ترتیب بیش از ۲۰ و ۱۲ میلیون دلار جمع‌آوری نمود. Pebble توسط Fitbit در سال ۲۰۱۶ به مبلغ ۲۳ میلیون دلار خریداری شد.

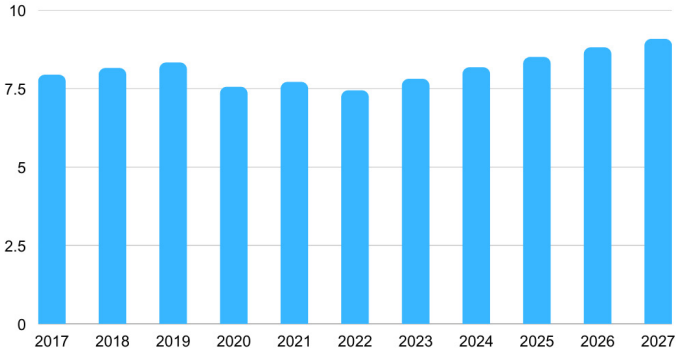
Glowforge: یک چاپگر لیزری سه‌بعدی با تکنولوژی بالاست که به افراد اجازه می‌دهد همه‌چیز از چرم گرفته تا پلاستیک را برای تولید محصول استفاده کنند. این شرکت در سال ۲۰۱۵ کمپین سرمایه‌گذاری جمعی را برای جمع‌آوری ۱۰۰ هزار دلار راه‌اندازی کرد، اما رکوردها را شکست و در یک ماه ۲۷٫۹ میلیون دلار جمع‌آوری کرد. این کمپین در طول اجرا، محصول مورد نظر را با تخفیف قابل توجهی عرضه کرد که بیش از ۱۰هزار حامی را جذب نمود. Glowforge تا به امروز بیش از ۲۵ هزار دستگاه را ارسال کرده و نظرات مثبتی از مشتریان خود دریافت نموده است.

تامین مالی جمعی در جهان

در حال حاضر، بازار تامین مالی جمعی مبتنی بر پاداش، رشد ثابتی را تجربه می‌کند، زیرا کارآفرینان و هنرمندان بیشتری به تامین مالی جمعی به عنوان ابزاری برای تأمین مالی پروژه‌های خود روی می‌آورند. پیش‌بینی‌ها نشان می‌دهند که بازار تامین مالی جمعی تا سال ۲۰۲۷، افزایش ملایمی را تجربه خواهد کرد (شکل ۱ و ۲). همه‌گیری COVID-۱۹ روند جذب سرمایه آنلاین را تسریع کرده، زیرا افراد بیشتری برای حمایت از کسب‌وکارهای کوچک و کارآفرینان مستقلی که تحت تأثیر قرنطینه‌ها و رکود اقتصادی قرار گرفته‌اند، از تامین مالی جمعی استقبال کرده‌اند. برای مثال، در



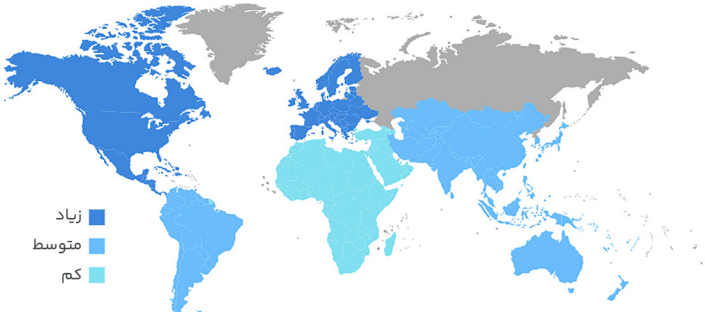
شکل ۱: ارزش معاملات در بازار تامین مالی جمعی جهان در سال‌های مختلف (برحسب میلیارد دلار)



شکل ۲: میانگین سرمایه‌گذاری در هر کمپین تامین مالی جمعی در سال‌های مختلف (برحسب هزار دلار)

آوریل ۲۰۲۱، Ketto، بیش از ۱۳۹ میلیون دلار در تلاش‌های مربوط به کووید جمع‌آوری کرد و در آوریل ۲۰۲۰، فیس‌بوک یک برنامه برای کمک خیریه برای بیماران درگیر کووید راه‌اندازی نمود. افزایش فعالیت‌های تامین مالی جمعی در پلتفرم‌های رسانه‌های اجتماعی، نقشی حیاتی در افزایش تقاضا برای پروژه‌های تامین مالی جمعی آتی دارد. پلتفرم‌های رسانه‌های اجتماعی مانند توییتر، فیس‌بوک، لینکدین، ردیت و اینستاگرام برای فعالیت‌های تامین مالی جمعی محبوبیت بیشتری دارند. برای مثال، ۳ درصد از اشتراک‌گذاری‌های توییتر، ۱۲ درصد از اشتراک‌گذاری‌های فیس‌بوک و ۵۳ درصد از اشتراک‌گذاری‌های ایمیل به کمک مالی تبدیل می‌شوند.

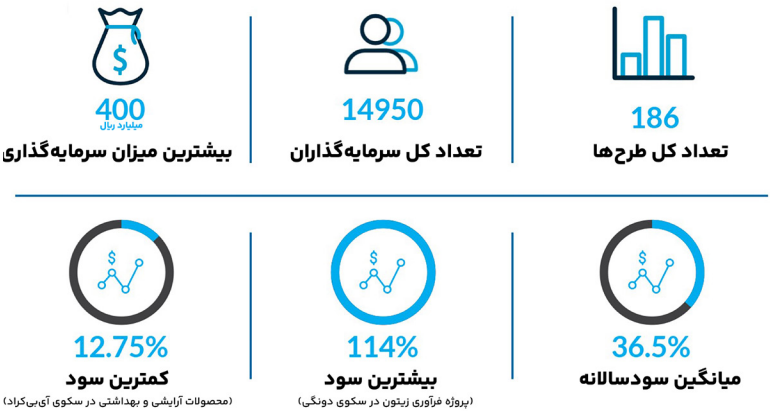
بر اساس نرخ رشد فعلی بازار تامین مالی جمعی، انتظار می‌رود آمریکای شمالی همچنان، بر این بازار تسلط داشته باشد (شکل ۳). افزایش تعداد شرکت‌های نوپا در سراسر این منطقه باعث رشد بازار آن می‌شود. همچنین پیش‌بینی می‌شود آسیا و اقیانوسیه، نرخ رشد سریعی را تجربه کنند. افزایش تعداد کسب‌وکارها، پروژه‌های نوآورانه و افزایش نفوذ اینترنت در سراسر این منطقه که منجر به دسترسی بهتر به پلتفرم‌ها را می‌گردد، از جمله عوامل اصلی رشد آن‌ها هستند. انتظار می‌رود تامین مالی جمعی فناوری در ژاپن محبوبیت پیدا کند. همچنین تعداد فزاینده استارت‌آپ‌ها در آمریکای جنوبی فرصت‌های گسترده‌ای را در بازار ایجاد می‌کند. از طرفی انتظار می‌رود اروپا در آینده نرخ رشد ثابتی را به دلیل افزایش تعداد دستورالعمل‌ها برای مدل تامین مالی جمعی تجربه کند. توسعه فناوری‌های جدید و تعداد فزاینده شرکت‌های فناوری در این منطقه، فرصت‌های سودآور جدیدی را در حوزه املاک، بانکداری و سایر صنایع فراهم کرده است. کشورهای اتحادیه اروپا ظاهراً قصد دارند قوانینی را وضع کنند که فعالیت سایت‌های تأمین مالی جمعی را در سایر مناطق اتحادیه اروپا امکان‌پذیر کنند. پلتفرم های مختلف تامین مالی جمعی در آلمان به سرمایه‌گذاران تازه‌کار و با تجربه امکان دسترسی به فرصت‌های سرمایه‌گذاری خصوصی را می‌دهند. سایت‌های جمع‌سپاری آلمانی جزو منظم‌ترین سایت‌ها بوده و به بهترین شیوه‌نامه‌ها پایبند هستند. بنابراین آلمان یک بازار کلیدی برای تامین مالی جمعی است. بازار سرمایه‌گذاری جمعی اروپا اخیراً پیشرفت‌های چشمگیری داشته است. به عنوان مثال، در آوریل امسال، دومین کمپین سرمایه‌گذاری جمعی Heura، تنها در ۱۲ ساعت، تقریباً ۴٫۲۲ میلیون دلار جمع‌آوری کرد و کمپین Crowdcube باعث شد ۴۵۰۰ سرمایه‌گذار از سراسر اروپا به انجمن Good Rebel ملحق شوند که مسئول پروژه سرعت بخشیدن به انتقال پروتئین است.



شکل ۳: نرخ رشد بازار تامین مالی جمعی در نواحی مختلف جهان

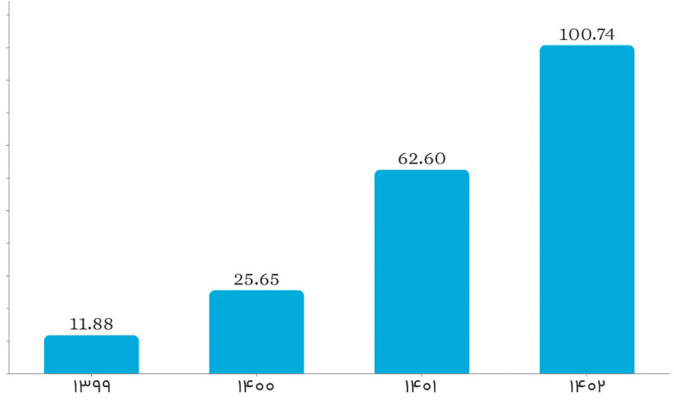
تامین مالی جمعی در ایران

در ایران، تامین مالی صنایع و بنگاه‌های اقتصادی عمدتاً از طریق سیستم بانکی انجام می‌شود. شرکت‌های بزرگ که سابقه و رتبه اعتباری مناسبی در سیستم بانکی دارند، مشکل کمتری در جهت اخذ وام دارند؛ اما برای شرکت‌های کوچک و متوسط که تقریبا ۹۰ درصد صنایع کشور را تشکیل می‌دهند، تامین مالی و اخذ وام بسیار دشوار است. شرکت‌های کوچک و متوسط برای رقابت، نوآوری و شکوفایی کشورها ضروری هستند و سهم قابل توجهی در تولید ناخالص داخلی آن‌ها و همچنین ایجاد فرصت‌های شغلی متعدد دارند؛ اما عدم حمایت از آن‌ها در تامین منابع مالی لازم، دلیل اصلی کوچک‌ماندن سهم این شرکت‌ها در اقتصاد ایران است. براساس گزارش‌های وزارت صنعت، معدن و تجارت، در سال ۱۴۰۰ کمتر از ۴درصد کل تقاضاهای وام صنایع اجابت شده است. همچنین به دلیل وجود تورم و نیاز شدید به سرمایه در گردش در بنگاهای کوچک و متوسط، تقاضا برای تسهیلات در سال ۱۴۰۱ افزایش داشته و به رقمی نزدیک به ۱۲هزار و ۸۰۰میلیارد تومان رسیده که نظام بانکی کشور به کمتر از یک ششم آن‌ها تسهیلات پرداخته است. از این رو، ایجاد سایر ابزارهای تامین مالی مانند تامین مالی جمعی و تقویت آن‌ها برای برآورده‌کردن این تقاضاها حائز اهمیت است. ارکان اصلی تامین مالی جمعی در ایران شامل پنج رکن به شرح ذیل است: متقاضی تامین مالی؛ توده مردم به عنوان تامین‌کنندگان مالی (سرمایه‌گذاران خرد شامل اشخاص حقیقی و حقوقی)؛پلتفرمی که زمینه ارتباط میان متقاضی و سرمایه‌گذاران خرد را فراهم

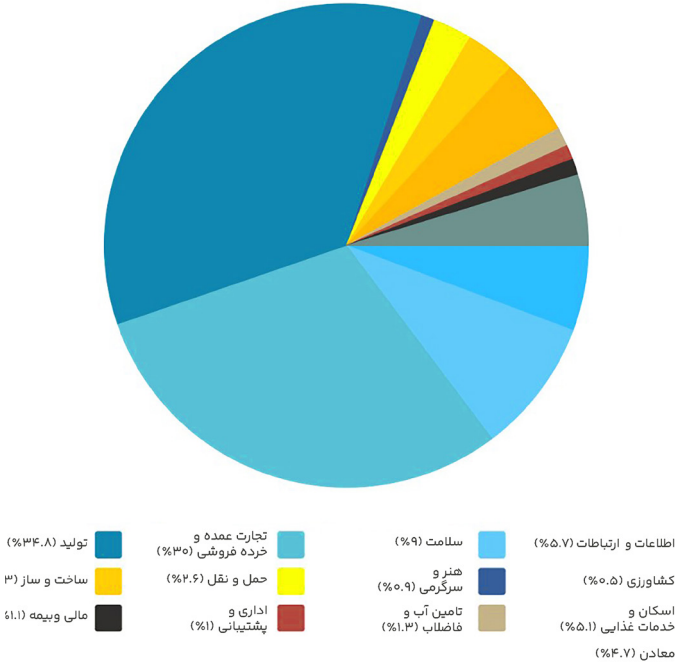


شکل ۴: آمار کلی عملکرد تامین مالی جمعی در ایران تا خرداد ۱۴۰۲ (منبع غیررسمی)

می‌کند (عامل یا سکو)؛ نهاد قانون‌گذار (سازمان فرابورس)؛ ناظر فنی/مالی. همچنین فرآیند تامین مالی، هفت مرحله شامل ۱) یافتن متقاضی تامین مالی (منبع‌یابی)، ۲) ارزیابی طرح متقاضی توسط عامل یا ناظر فنی/مالی، ۳) پذیرش و عقد قرارداد عامل با متقاضی تامین مالی جمعی، ۴) دریافت نماد اختصاصی از فرابورس، ۵) انتشار فراخوان جذب سرمایه، ۶) آغاز طرح در صورت موفقیت پویش و ۷) پایان طرح و تسویه دارد.



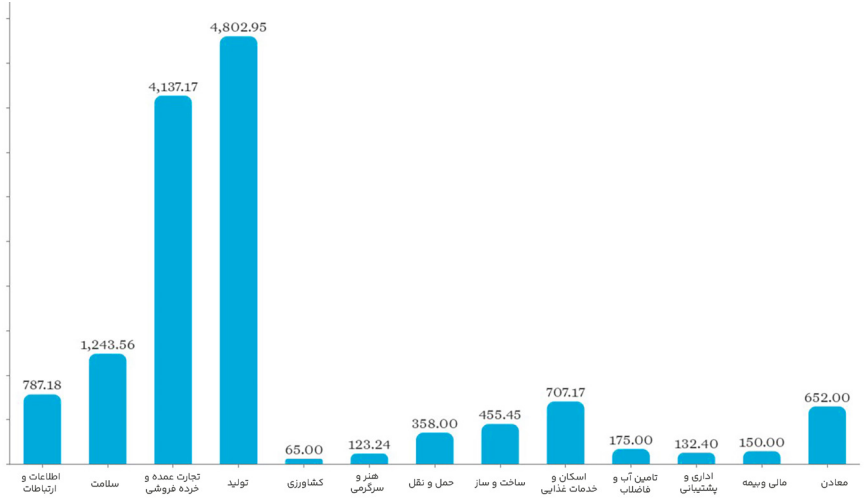
شکل ۵: حجم سرمایه جمع‌آوری شده از طریق تامین مالی جمعی در هرسال برحسب میلیارد ریال



شکل ۶: سهم حوزه‌های مختلف در بازار تامین مالی ایران

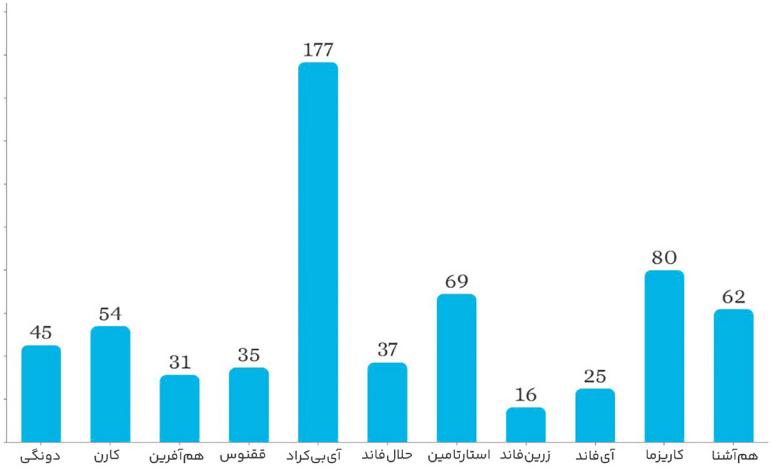
تامین مالی جمعی در ایران توسط شرکت فرابورس ایران مقررات‌گذاری شده و این نهاد به سکوها مجوز اعطا می‌کند. البته مجوز فرابورس صرفاً برای تامین مالی جمعی مبتنی بر سهام است. سرمایه‌گذار در این مدل، دارنده گواهی مشارکت است که سهمی از پروژه تعریف‌شده دارد. ویژگی‌های تامین مالی جمعی مبتنی بر سهام در ایران شامل موارد زیر است:

سقف تامین مالی جمعی تا ۲۵ میلیارد تومان، تشریفات کمتر نسبت به روش‌های دیگر تامین مالی بازار سرمایه (حدوداً ۲ ماه)، پرداخت سود در طول دوره و پرداخت اصل در انتهای دوره (جذاب‌ترین ویژگی این نوع تامین مالی نسبت به بانک)، عدم نیاز به وثایق، نرخ تامین مالی حدود ۱۰ درصد بالاتر از نرخ بانکی، سرعت در تامین مالی، تامین‌کننده منابع، نقش مشارکت‌کننده در طرح را داشته و در سود و زیان طرح شریک است، معافیت مالیاتی برای تامین‌کنندگان منابع، امکان مشارکت سرمایه‌گذاران خرد، تامین مالی کوتاه‌مدت. در نهایت اگر در شرکتی، پروژه سوددهی تعریف شود که زیر ۲۵ میلیارد تومان به سرمایه نیاز داشته باشد و بتواند حداکثر تا دو سال آن را تسویه نماید، می‌تواند از تامین مالی جمعی استفاده کند. همچنین الزامات تامین مالی از طریق سکوها به صورت موارد زیر تعریف می‌شود: اطلاعات ثبتی شرکت، طرح توجیهی اقتصادی، صورت‌های مالی دو سال اخیر، ضمانت‌نامه بانک/صندوق پژوهش‌وفناوری.



شکل ۷: حجم سرمایه جمع‌آوری‌شده در حوزه‌های مختلف تامین مالی جمعی ایران (برحسب میلیارد ریال)

از زمان تصویب مجوز تامین مالی جمعی در ایران توسط شورای عالی بورس و اوراق بهادار در سال ۱۳۹۷، تاکنون ۲۱ سکو موفق به اخذ مجوز شده‌اند که مجوز ۳ مورد از آن‌ها لغو شده و اکنون ۱۸ سکو فعال هستند (شکل ۴). شکل‌های ۵ تا ۸ حاصل تحلیل اینوستک از داده‌های سازمان فرابورس برای تامین مالی جمعی در ایران از ابتدای سال ۱۳۹۹ تا ۱۹ مردادماه ۱۴۰۲ و برای ۱۱ سکوست که حوزه‌های فعالیت آن‌ها بر اساس استاندارد جهانی ISIC دسته‌بندی شده‌اند. بر این اساس، حجم کل تامین مالی جمعی برابر با ۱۳ هزار میلیارد ریال و درصد موفقیت کمپین‌ها، ۹۵ درصد بدست آمده است. شکل ۵، حجم سرمایه تامین‌شده در هر سال را نمایش می‌دهد که نشانگر رشد میزان تامین مالی جمعی است. همچنین در شکل ۸، میزان سرمایه تامین‌شده توسط هر سکو نمایش داده شده که طبق آن، سکوی آی‌بی‌کراد با ۱۷۷ میلیارد ریال پیشگام است. درصد سهم هر حوزه از میزان کل سرمایه‌گذاری‌ها و حجم سرمایه تامین‌شده در هر حوزه به ترتیب در شکل‌های ۶ و ۷ نمایش داده شده‌اند. در فضای اقتصادی کشور که تنها ۱۰ درصد از کل صادرات کشور به شرکت های کوچک و متوسط اختصاص دارد، با بهره گیری مناسب از بستر ایجادشده توسط سکوهای تامین مالی جمعی می توان ظرفیت‌های نهفته در شرکت‌های کوچک و متوسط را در جهت صادرات تقویت کرد و در جهت توسعه اقتصاد کشور قدم برداشت.



شکل ۸: حجم سرمایه جمع‌آوری‌شده در سکوهای مختلف تامین مالی جمعی ایران (برحسب میلیارد ریال)


امنیت سایبری:
پانهادن در
میدان مین
دنیای دیجیتال

امنیت سایبری عمل دفاع از رایانه‌ها، سرورها، دستگاه‌های تلفن همراه، سیستم‌های الکترونیکی، شبکه‌ها و داده‌ها در برابر حملات دیجیتال و دسترسی‌های غیرمجاز است. اقدامات امنیت سایبری که به عنوان امنیت فناوری اطلاعات (IT) یا سایبرتک نیز شناخته می‌شوند، برای مقابله با تهدیدات علیه سیستم‌ها و برنامه‌های شبکه‌ای طراحی شده‌اند، فارغ از اینکه این تهدیدات از کجا سرچشمه می‌گیرند. امنیت سایبری تمام کسانی که از اینترنت استفاده می‌کنند را تحت تاثیر قرار می‌دهد، اما اغلب توسط بسیاری از مردم نادیده گرفته می‌شود. حملات سایبری اشکال مختلفی داشته و می‌توانند منجر به عواقب جدی مانند خسارات مالی، سرقت هویت، آسیب به شهرت، مسئولیت قانونی و حتی آسیب فیزیکی برای افراد و سازمان‌ها شوند. اهمیت امنیت سایبری در دنیای دیجیتال امروزی قابل چشم‌پوشی نیست. طبق گزارش Cybersecurity Ventures، انتظار می‌رود تا سال ۲۰۲۵، جرایم سایبری سالانه ۱۰٫۵ تریلیون دلار برای جهان هزینه داشته باشد که این رقم در سال ۲۰۱۵، ۳ تریلیون دلار بود (شکل ۹). این بدان معناست که هر ۱۱ ثانیه، یک تجارت، قربانی یک حمله سایبری می‌شود. علاوه بر این، حملات سایبری پیچیده‌تر و هدفمندتر می‌شوند، زیرا هکرها از تکنیک‌ها و ابزارهای پیشرفته برای سوء استفاده از آسیب‌پذیری‌ها در سیستم‌ها و رفتار انسانی استفاده می‌کنند. یک راهبرد قوی امنیت سایبری می‌تواند امنیت خوبی در برابر حملات مخرب ایجاد کند که برای دسترسی، تغییر، حذف، تخریب داده‌ها یا اخاذی از سازمان یا کاربر طراحی شده‌اند. اهمیت امنیت سایبری با افزایش تعداد کاربران، دستگاه‌ها و برنامه‌ها در شرکت‌های مدرن، و افزایش سیل داده‌ها – که بیشتر آنها حساس یا محرمانه هستند – در حال افزایش است. حجم فزاینده و پیچیدگی مهاجمان سایبری و تکنیک‌های حمله، این مشکل را حتی بیشتر می کند .

تهدیدات رایج

اگرچه متخصصان امنیت سایبری سخت تلاش می‌کنند تا شکاف‌های امنیتی را ببندند، اما مهاجمان همیشه به دنبال راه‌های جدیدی برای فرار از اقدامات دفاعی و سوء استفاده از نقاط ضعف در حال ظهور هستند. رایج‌ترین تهدیدات سایبری عبارتند از: **بدافزار (Malware):** اصطلاح «بدافزار» به انواع نرم‌افزارهای

مخرب - مانند کرم‌ها، ویروس‌ها، تروجان‌ها و جاسوس‌افزارها اشاره دارد که دسترسی غیرمجاز را ممکن کرده یا به رایانه آسیب می‌رسانند.

باج‌افزار(Ransomware): باج‌افزار نوعی بدافزار است که فایل‌ها، داده‌ها یا سیستم‌ها را قفل کرده و تهدید می‌کند که داده‌ها را پاک یا نابود می‌نماید - یا داده‌های خصوصی یا حساس را در اختیار عموم قرار می‌دهد - مگر اینکه به مجرمان سایبری که حمله را انجام داده‌اند، باج پرداخت شود.

فیشینگ/مهندسی اجتماعی (Phishing): فیشینگ نوعی مهندسی اجتماعی است که کاربران را فریب می‌دهد تا اطلاعات حساس خود را ارائه دهند. در کلاهبرداری‌های فیشینگ، به نظر می‌رسد ایمیل‌ها یا پیام‌های متنی، از طرف یک شرکت قانونی است که اطلاعات حساسی مانند اطلاعات کارت اعتباری یا اطلاعات ورود به سیستم را درخواست می‌کند.

حمله توزیع‌شده انکار سرویس (DDoS): یک حمله DDoS سعی می‌کند یک سرور، وب‌سایت یا شبکه را با بارگذاری بیش از حد ترافیک خراب کند. حملات DDoS از طریق پروتکل ساده مدیریت شبکه (SNMP) که برای مودم‌ها، چاپگرها، سوئیچ‌ها، روترها و سرورها استفاده می‌شود، بر شبکه‌های سازمانی غلبه می‌کند.

تهدیدات پایدار پیشرفته (APT): در یک APT، یک مزاحم یا گروهی از متجاوزان به یک سیستم نفوذ می‌کنند و برای مدت طولانی شناسایی نمی‌شوند. نفوذگر، شبکه‌ها و سیستم‌ها را دست‌نخورده رها می‌کند تا بتواند از فعالیت‌های تجاری جاسوسی کند و داده‌های حساس را بدزدد و در عین حال از فعال‌سازی اقدامات دفاعی اجتناب کند.

حمله مرد میانی (Man-in-the-Middle): یک حمله از نوع شنود است که در آن یک مجرم سایبری، پیام‌ها را بین دو طرف مکالمه، رهگیری و ارسال می‌کند تا داده‌ها را بدزدد.

تهدیدات داخلی کارمندان فعلی یا سابق، شرکای تجاری، پیمانکاران، یا هرکسی که در گذشته به سیستم‌ها یا شبکه‌ها دسترسی داشته است، در صورت سوءاستفاده از مجوزهای دسترسی، می‌تواند به عنوان یک تهدید داخلی در نظر گرفته شود.

تصورات اشتباه در امنیت سایبری

حجم حوادث امنیت سایبری در سرتاسر جهان در حال افزایش است، اما تصورات غلط همچنان پابرجاست، مهم‌ترین آن‌ها عبارتند از:

- مجرمان سایبری خارجی هستند. در واقعیت، نقض امنیت سایبری اغلب توسط افراد خرابکار داخلی که برای خودشان یا با همکاری هکرهای خارجی کار می‌کنند، اتفاق می‌افتد. این خودی‌ها می‌توانند بخشی از گروه‌های سازمان‌یافته و تحت حمایت دولت‌ها باشند.

– خطرات به خوبی شناخته شده‌اند. در واقع، سطح خطر همچنان در حال گسترش است و هزاران آسیب‌پذیری جدید در برنامه‌ها و دستگاه‌های جدید و قدیمی گزارش شده است.

– صنعت من، امن است. هر صنعتی به نوبه خود سهمی از خطرات امنیت سایبری دارد، به طوری که خرابکاران سایبری از نیازهای شبکه‌های ارتباطی تقریباً در هر سازمان دولتی و بخش خصوصی سوء استفاده می‌کنند.

خدمات امنیت سایبری

ارائه‌دهندگان خدمات امنیت سایبری معمولاً محصولات و خدمات امنیتی مختلفی ارائه می‌دهند که رایج‌ترین آن‌ها عبارتند از:

مدیریت هویت و دسترسی (IAM)، فایروال‌ها، حفاظت نقطه پایانی، آنتی‌بدافزار/آنتی‌ویروس، سیستم‌های پیشگیری/تشخیص نفوذ (IPS/IDS)، پیشگیری از از دست‌رفتن داده‌ها (DLP)، تشخیص و پاسخ نقطه پایانی، اطلاعات امنیتی و مدیریت رویداد (SIEM)، ابزارهای رمزگذاری، اسکنرهای آسیب پذیری، شبکه‌های خصوصی مجازی (VPN)، پلتفرم حفاظت از بار کاری ابری (CWPP)و کارگزار امنیت دسترسی ابری (CASB).

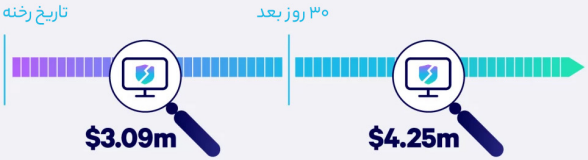
همچنین MSSP مخفف Managed Security Service Provider و به معنای «ارائه‌دهنده خدمات امنیتی مدیریت‌شده»، نوعی شرکت است که راه‌حل‌های امنیتی برون‌سپاری را به سایر سازمان‌ها ارائه می‌دهد. MSSPها می‌توانند با ارائه خدماتی مانند مدیریت فایروال، تشخیص نفوذ، پیکربندی VPN، اسکن آسیب‌پذیری و آنتی‌ویروس، به مشتریان خود در محافظت از شبکه‌ها، سیستم‌ها، دستگاه‌ها و داده‌ها در برابر تهدیدات سایبری کمک کنند. یک سازمان با به کارگیری MSSP می‌تواند از چندین مزیت، مانند تکمیل تیم امنیت داخلی خود، دسترسی به متخصص و کاهش هزینه‌ها و خطرات بهره‌مند شود. MSSPها همچنین می‌توانند با تغییر نیازها و چالش‌های مشتریان خود، مانند پشتیبانی از زیرساخت‌های مبتنی بر آبر یا پاسخ به انواع جدید حملات، سازگار شوند. MSSPها با MSPها (Managed Service Providers) که پشتیبانی عمومی از شبکه و فناوری اطلاعات را ارائه می‌دهند و بر امنیت تمرکز ندارند، متفاوت هستند.

شکل۹: میزان رشد هزینه‌های جرایم سایبری

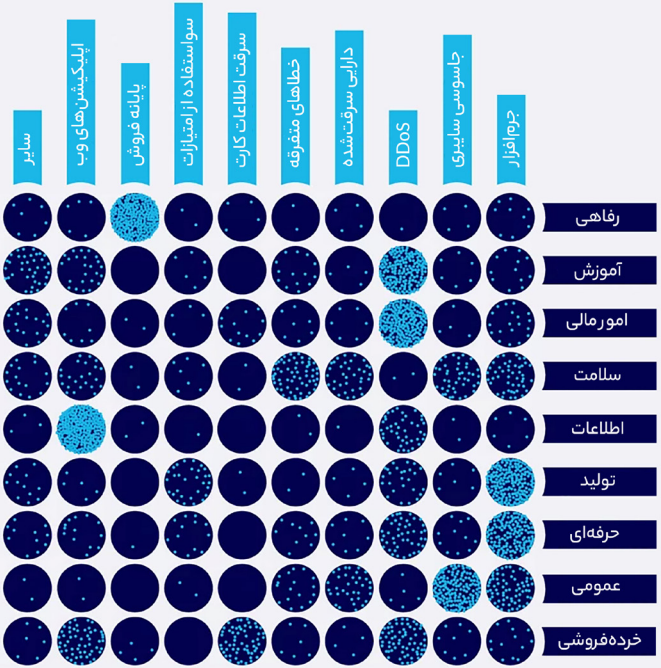
آمار امنیت سایبری

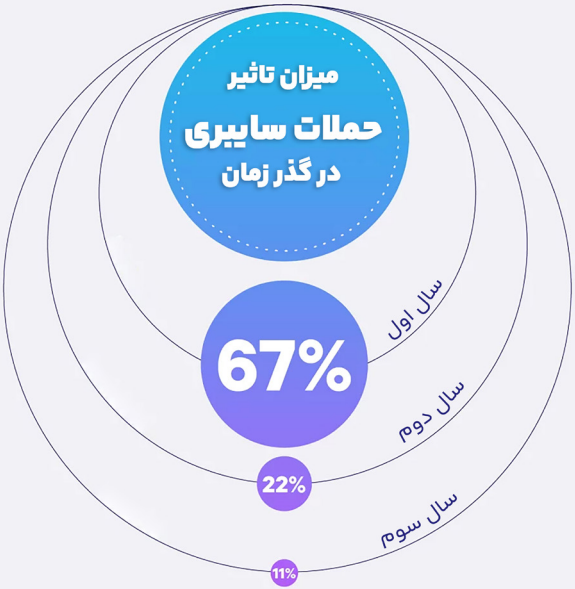
فرکانس حملات باج‌افزاری

کشف یک رخنه به طور متوسط ۱۹۷ روز طول می‌کشد



حوادث سایبری در صنعت‌های مختلف

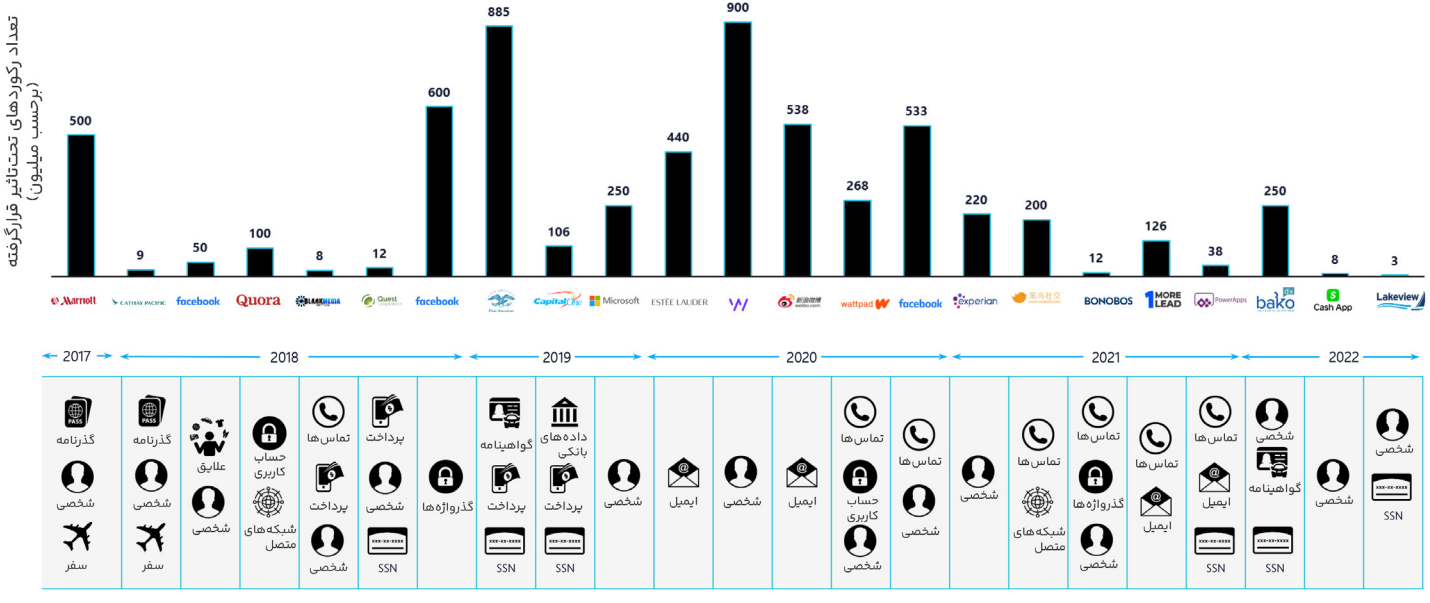




این داده‌ها شامل هزینه‌های از دست رفتن داده، ورشکستگی کسب‌وکار، سودهای ازدست رفته به خاطر قطعی سیستم، هزینه‌های اطلاع‌رسانی و آسیب به اعتبار شرکت و هزینه ازدست رفتن مشتریان است.

چه کسانی منجر به نشت داده‌ها می‌شوند؟

سیر زمانی نشت‌های مهم داده در جهان از سال ۲۰۱۷



سیرزمانی حملات سایبری مهم احتمالی در ایران از سال ۱۴۰۰

اسفند ۱۴۰۰

- وزارت فرهنگ و ارشاد اسلامی

بهمن ۱۴۰۰

- صدا و سیمای جمهوری اسلامی ایران
- سامانه تلوبیون
- زندان قزلحصار

آبان ۱۴۰۰

- سامانه کارت سوخت
- شرکت ملی گاز ایران
- شرکت هواپیمایی ماهان

مرداد ۱۴۰۰

- زندان اوین

تیر ۱۴۰۰

- راه‌آهن جمهوری اسلامی ایران
- پورتال وزارت راه

فرودین ۱۴۰۰

- تجهیزات هسته‌ای نطنز

آبان ۱۴۰۱

- کارگروه تعیین مصادیق مجرمانه

مهر ۱۴۰۱

- آستان قدس رضوی
- صدا و سیما
- سازمان انرژی اتمی
- وزارت کار
- نیروگاه هسته‌ای بوشهر

شهریور ۱۴۰۱

- پایگاه اطلاع‌رسانی دولت
- درگاه ملی دولت هوشمند
- بانک مرکزی ایران
- وزارت فرهنگ و ارشاد اسلامی
- خبرگزاری فارس

تیر ۱۴۰۱

- شرکت فولاد خوزستان
- شرکت فولاد مبارکه اصفهان
- سازمان فرهنگ و ارتباطات اسلامی

خرداد ۱۴۰۱

- شهرداری تهران

اردیبهشت ۱۴۰۱

- وزارت جهاد کشاورزی

شهریور ۱۴۰۲

- تپسی
- شرکت‌های بیمه

خرداد ۱۴۰۲

- افتای ریاست جمهوری

اردیبهشت ۱۴۰۲

- وزرات امور خارجه

بهمن ۱۴۰۱

- اینترنت سراسری کشور (ارتباطات زیرساخت)
- زندان اوین

دی ۱۴۰۱

- پیام‌رسانهای ایرانی
- دانشگاه امام صادق

آذر ۱۴۰۱

- وب‌سایت خبرگزاری فارس
- دانشگاه الزهرا
- دانشگاه خواجه نصیر

آمار کلی جرایم سایبری تا سال ۲۰۲۲

۳۷ قربانی در هر ثانیه

میانگین ۹۷ قربانی جرایم سایبری در ساعت، بدان معناست که هر ۳۷ ثانیه، یک نفر قربانی جرایم سایبری می شود.

۲ کاربر در هر ثانیه

در سال ۲۰۲۲ در هر ثانیه، اطلاعات ۲ کاربر اینترنت درز کرد که نسبت به سال ۲۰۲۱ (هر ثانیه ۶ کاربر) سه برابر شد.

$4.35 M

در سال ۲۰۲۲ نقض داده‌ها به طور متوسط ۴.۳۵ میلیون دلار برای کسب و کارها هزینه داشت.

$6 B

جرایم سایبری در سال ۲۰۲۱ حدود ۶ میلیارد دلار در یکسال برای اقتصادهای جهانی هزینه داشت.

100%

کمترین آسیب جرایم سایبری متوجه افراد زیر ۲۰سال است، اما افزایش تحصیل آنلاین در دوره پاندمی در سال ۲۰۲۰، منجر به افزایش تقریباً ۱۰۰% این قربانیان شد.

55%

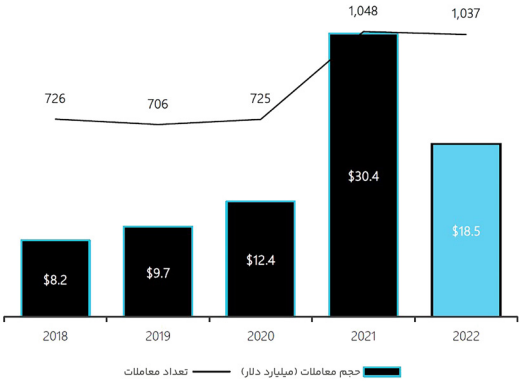
بازنشستگان (بالای ۶۰سال) آسیب‌پذیرترین گروه در برابر جرایم سایبری هستند. در سال ۲۰۲۰ تعداد این قربانیان، ۵۵ درصد افزایش یافت و تا سال ۲۰۲۱به بیش از ۹۲ هزار رسید.

سهم حوزه‌های مختلف در بازار کل امنیت جهانی (۱.۵ تا ۲ تریلیون)

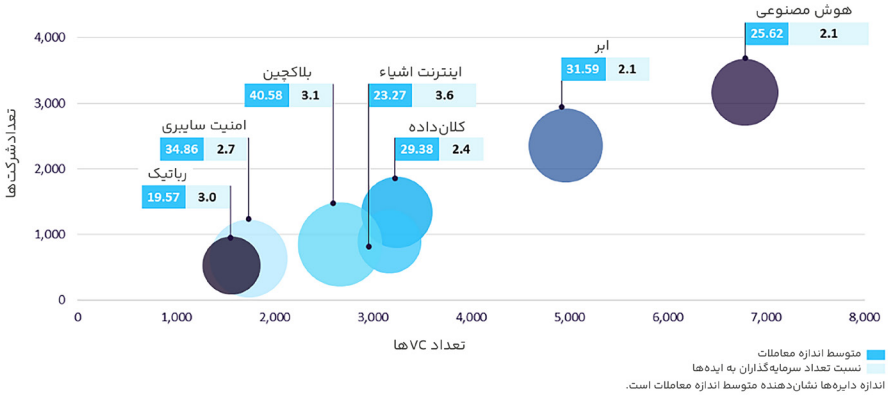
حوزه	بازار کل (بر حسب میلیارد دلار)
مشاوره امنیت	100–200
امنیت وب	100–200
اینترنت اشیاء / فناوری عملیاتی	100–200
امنیت نقطه پایانی	100–200
امنیت اپلیکیشن	100–200
مدیریت عملیات و هویت	400–500
MSSP*/برون‌سپاری	400–500
حفاظت داده	50–100
حاکمیت، ریسک و انطباق	50–100
امنیت ایمیل	50–100
امنیت ابری	50–100
امنیت شبکه	50–100
مدیریت دسترسی و هویت	50–100

*ارائه‌دهنده خدمات امنیتی مدیریت‌شده

سرمایه‌گذاری سالانه در امنیت سایبری



چشم‌انداز سرمایه‌گذاری خطرپذیر (VC) در فناوری‌های انقلابی در سال ۲۰۲۱



دیپ‌وب و دارک‌وب: شیرجه در عمق تاریک اینترنت

اینترنت مانند یک کوه یخ است: آنچه در سطح می‌بینیم تنها کسری از چیزی است که در زیر آن نهفته است. بسیاری از ما با بخشی از اینترنت که توسط مرورگرها و موتورهای جستجوی استاندارد قابل دسترسی است، آشناییم. این بخش، وب سطحی (Surface Web) نام داشته و تنها حدود ۱۰ درصد اطلاعات موجود در اینترنت را تشکیل می‌دهد. بخش دیگر و بزرگ‌تری از اینترنت وجود دارد که از دید عموم پنهان است. این بخش که دیپ‌وب (Deep Wb) نام دارد، توسط موتورهای جستجوی معمولی نمایه نمی‌شود و بنابراین برای دسترسی به آن، ابزارها یا روش‌های خاصی لازم است. دیپ‌وب حاوی حجم وسیعی از اطلاعات است، از پایگاه‌های اطلاعاتی دانشگاهی و سوابق دولتی گرفته تا ایمیل‌های شخصی و حساب‌های رسانه‌های اجتماعی. آمارها حاکی از آن است که دیپ‌وب ۴۰۰ تا ۵۵۰ برابر بزرگ‌تر از وبِ قابل مشاهده است. با این همه، در دیپ‌وب قلمرویی حتی تاریک‌تر و مرموزتر، به نام دارک‌وب (Dark Web) وجود دارد. دارک‌وب بخشی از اینترنت است که به طور عمدی پنهان و رمزگذاری‌شده و تنها با استفاده از نرم‌افزارهای خاصی مانند Tor می‌توان به آن دسترسی داشت. در دارک‌وب اغلب فعالیت‌های غیرقانونی مانند قاچاق مواد مخدر، هک، جرایم سایبری، تروریسم و قاچاق انسان جریان دارد. دارک‌وب همچنین میزبان سایت‌های مختلفی است که خدمات یا محتوایی را ارائه می‌دهند که تابو، غیراخلاقی یا بحث‌انگیز تلقی می‌شوند، مانند پلتفرم‌های افشاگر، مخالفان سیاسی، گروه‌های افراطی یا هرزه‌نگاری. دارک‌وب مکانی است که در آن حریم خصوصی بیش از هر چیزی ارزش دارد، با این حال، خطر و فریب در هر گوشه‌ی آن در کمین است. شباهت دیپ‌وب و دارک‌وب در این است که هیچ‌یک توسط موتورهای جستجوی معمولی نمایه نمی‌شوند، با این حال دیپ‌وب به مرورگر خاصی هم نیاز ندارد، اما دسترسی به دارک‌وب نیازمند مرورگر خاصی مانند Tor است.

چند نمونه دیپ‌وب

ایمیل‌وب: سرویس‌های پست الکترونیکی وب، مانند Gmail، Yahoo Mail یا Outlook، ایمیل‌های شما را در سرورهای خود ذخیره می‌کنند که توسط موتورهای جستجو قابل دسترسی نیستند. برای مشاهده ایمیل‌های خود باید با نام کاربری و رمز عبور وارد شوید. **بانکداری آنلاین:** خدمات بانکداری آنلاین، به شما امکان می‌دهند امور مالی خود را به صورت آنلاین مدیریت کنید. برای دسترسی به حساب بانکی خود باید شماره حساب و رمز عبور خود را وارد کنید. **فضای ذخیره‌سازی ابری:** سرویس‌های

ذخیره‌سازی ابری مانند Google Drive، Dropbox یا OneDrive به شما امکان می‌دهند فایل‌های خود را به صورت آنلاین ذخیره کنید. شما برای دسترسی به فایل‌های خود باید با ایمیل و رمز عبور وارد شوید. **محتوای خدمات درازای هزینه:** محتوای خدمات در ازای هزینه به وب‌سایت‌هایی اطلاق می‌شود که برای دسترسی به محتوای خود هزینه دریافت می‌کنند، مانند مجلات آنلاین، روزنامه‌ها، مجلات یا پایگاه‌های داده. شما برای دسترسی به محتوای آنها باید هزینه اشتراک بپردازید. **رسانه‌های اجتماعی با دسترسی محدود:** رسانه‌های اجتماعی با دسترسی محدود به وب‌سایت‌هایی اطلاق می‌شود که برای مشاهده محتوا نیاز به ثبت‌نام یا دعوت‌نامه دارند، مانند فیس‌بوک و توییتر. برای پیوستن به شبکه آنها باید یک حساب کاربری ایجاد کنید.

مزایای دیپ‌وب

حریم خصوصی: دیپ‌وب سطح بالاتری از حریم خصوصی را نسبت به وب سطحی ارائه می‌دهد، زیرا توسط موتورهای جستجو یا اشخاص ثالث ردیابی نمی‌شود. **امنیت:** دیپ‌وب نسبت به وب سطحی، امنیت بالاتری دارد، زیرا با روش‌های رمزگذاری و احراز هویت محافظت می‌شود. **اطلاعات:** دیپ‌وب حاوی حجم وسیعی از اطلاعات است که در سطح وب در دسترس نیستند، مانند پایگاه‌های اطلاعاتی دانشگاهی، سوابق دولتی و داده‌های علمی، بنابراین می‌توانید به اطلاعات قابل اعتمادتر و دقیق‌تری دسترسی داشته باشید.

چالش‌های دیپ‌وب

دسترسی: دیپ‌وب توسط مرورگرهای استاندارد و موتورهای جستجو به راحتی قابل دسترسی نیست. برای دسترسی به دیپ‌وب باید از ابزارها یا روش‌های خاصی استفاده کرد که ممکن است برای برخی کاربران پیچیده یا پرهزینه باشند. **کیفیت:** دیپ‌وب دارای محتوایی با طیف وسیعی از کیفیت و اعتبار است. برخی از وب‌سایت‌های موجود در دیپ‌وب ممکن است حاوی اطلاعات قدیمی، نادرست یا غیرقانونی باشند، بنابراین باید منبع و اعتبار اطلاعات را بررسی کنید. **اخلاق:** دیپ‌وب می‌تواند مسائل اخلاقی و قانونی برای کاربران خود ایجاد کند. برخی از وب‌سایت‌ها در دیپ‌وب ممکن است حقوق مالکیت معنوی، حقوق حریم خصوصی یا حقوق بشر را نقض کنند. شما باید از قوانین و مقرراتی که در مورد محتوای دیپ‌وب اعمال می‌شوند آگاه باشید.

چند نمونه دارک‌وب

DuckDuckGo موتور جستجویی که داده‌های شخصی شما را ردیابی یا جمع‌آوری نمی‌کند و یکی از محبوب‌ترین و در دسترس‌ترین سایت‌ها در دارک‌وب است. Hidden Wiki فهرستی از پیوندهای دارک‌وب که می‌تواند به شما در کشف دارک‌وب کمک کند و

شامل پیوندهایی به دسته‌های مختلف مانند بازارها، انجمن‌ها، میزبانی و ایمیل است. ProPublica یک پلتفرم روزنامه‌نگاری که داستان‌های تحقیقی و عمیق را در مورد موضوعاتی مانند سیاست، امور مالی، بهداشت، محیط زیست و موارد دیگر منتشر می‌کند و یکی از معدود خبرگزاری‌هایی است که دارای نسخه دارک‌وب برای محافظت از منابع و خوانندگان خود در برابر سانسور و نظارت است. Sci-Hub سایتی که به شما امکان دسترسی رایگان به میلیون‌ها مقاله علمی را داده و محدودیت‌های اعمال‌شده توسط ناشران دانشگاهی و مجلات را دور می‌زند. سای‌هاب یک وب‌سایت معمولی دارد که می‌توان از طریق هر مرورگری به آن دسترسی داشت، اما یک نسخه مخفی در دارک‌وب هم دارد. Hidden Answers بستری است که می‌توانید بدون سانسور یا اعتدال هر سوالی را درباره موضوعاتی چون فناوری، امنیت، مواد مخدر، سیاست و مذهب بپرسید یا پاسخ دهید.

خطرات دارک‌وب

دارک‌وب، مرکزی برای مجرمان سایبری و انجام فعالیت‌های غیرقانونی مانند هک، سرقت هویت، کلاهبرداری‌های فیشینگ و توزیع بدافزار است. بنابراین، اگر تصمیم به دسترسی به دارک‌وب دارید، باید اقدامات احتیاطی را برای محافظت از خود انجام دهید.

حقایق عجیب دارک‌وب

به طور غیرقابل باوری، ۸۰ درصد از بودجه Tor از سوی دولت آمریکا تامین می‌شود.

هزینه کشتن یک شخص معمولی ۲۰ هزار دلار و یک شخص مهم ۱۰۰ هزار دلار است.

ناشناس بودن دارک وب بستر مناسبی را برای کار هکرها فراهم می کند.

۶۰ وب‌سایت بزرگ دیپ دارای حدود ۷۵۰ ترابایت داده هستند، یعنی ۴۰ برابر بزرگتر از کل وب سطحی!

ادوارد اسنودن از دارک وب برای افشای فایل های مربوط به NSA استفاده کرد.

تخمین زده می‌شود که ۵۰ هزار گروه تروریستی افراطی در دارک وب وجود داشته باشد.

INVESTECH
nvest in Tech

با همکاریِ

FANASA
Research &Technology Fund

آدرس

نیاوران،کامرانیه‌شمالی،نبش
خیابان داریوش، پلاک ۲۹
برج پارادیس، واحد ۱

راه‌های ارتباطی

info@investech.fund
bale: @investech
021-2228-7541

WWW.INVESTECH.FUND
WWW.FANASAFUND.IR