گزارش سالانه باگدشت

۱۳۹۸

حفظ حریم خصوصی اطلاعات مشتریانتان برای شما دارای اهمیت است؟

به دنبال منابع جدید برای یافتن نقاط آسیب پذیر سامانه های خود هستید؟

برای اعتبار شهرت کسب و کار خود ارزش قایل هستید؟

یادداشت مدیریتی

هدف اصلی ایجاد پلتفرم های باگ بانتی این موضوع است که با کمک گرفتن از متخصصین متعهد، زمان دسترسی به مشکلات امنیتی سامانه های سازمانی را کوتاه نمایند و سازمان مخاطب اصلی باگ های امنیتی شود تا اگر این باگ توسط مهاجمین در حال استفاده می باشد، مدیران سازمان بتوانند سریعا مطلع و اقدامات ایمن سازی را صورت دهند.

همانطور که می دانیم، برخی از مهاجمین و متخصصین غیرمتعهد، بصورت مستمر در حال شناسایی و سواستفاده از باگ های امنیتی سامانه های سازمانی می باشند و با مبالغ مختلف به خرید فروش و یا کسب مزیت های شخصی می پردازند. در واقع باگ بانتی با کمک گرفتن از متخصصین امنیتی متعهد که هدف اجرای تخصصی امور امنیتی را در کشور دارند و ارایه انگیزه های تشویقی به آنها، محیطی برد برد برای دو سوی پلتفرم یعنی سازمان و متخصص ایجاد می نماید تا در نتیجه میزان نفوذ در کشور کاهش یابد.

مجموعه باگدشت با تکیه بر تجارب کارشناسان خود در کاربری پلتفرم های باگ بانتی بین المللی و همچنین اجرای پروژه های ارزیابی امنیتی و ایمن سازی مختلف در داخل کشور، در سال 1397 اقدام به شخصی سازی پلتفرم باگ بانتی ایرانی بصورت قانونی نمود و مفهوم باگ بانتی و باگ هانتینگ را ارایه کرد تا در نتیجه با عملیاتی شدن پروژه های امنیت و مقرون به صرف بودن آنها در برابر هزینه صورت گرفته کمک نماید و سازمانها بتوانند به باگ های امنیتی خود دسترسی یابند و به سرعت جهت ایمن سازی خود گام بردارند.

مساله اصلی در باگ بانتی ها شناسایی باگ نیست، مساله اساسی ایجاد فرآیندی بالغ در سازمانها برای ایمن سازی سریع است.

در این گزارش نگاهی اجمالی به یافته های متخصصین باگدشت در طول یک سال همکاری با کسب و کارهای متفاوت می پردازیم.

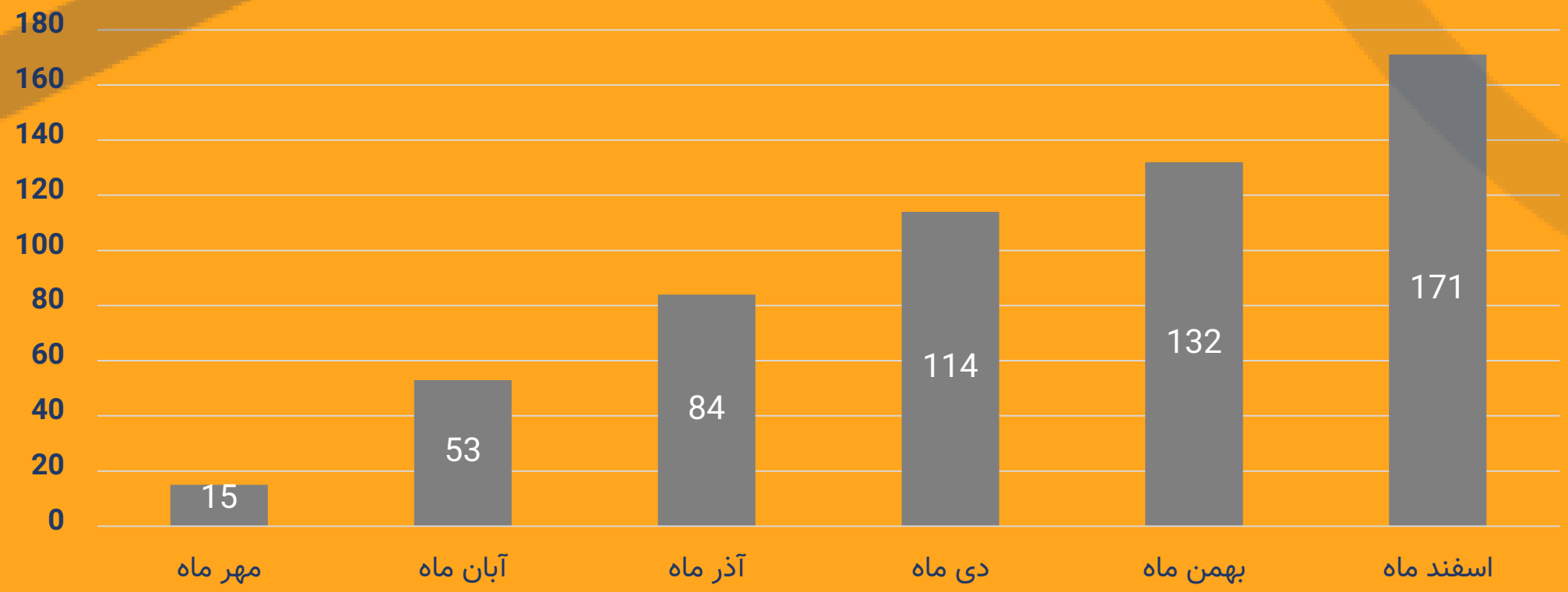
سرفصل مطالب

- عملکرد باگ بانتی باگدشت در سال گذشته؛ 6
- آمار و ارقام رخدادهای امنیتی بین المللی؛ 21
- راهکارهای ایمن سازی سامانه ها؛ 34
- تجربیات دیگر کشورها در باگ بانتی؛ 39
- مزیت استفاده از باگ بانتی؛ 46
- ملاحظات حقوقی باگ بانتی؛ 52

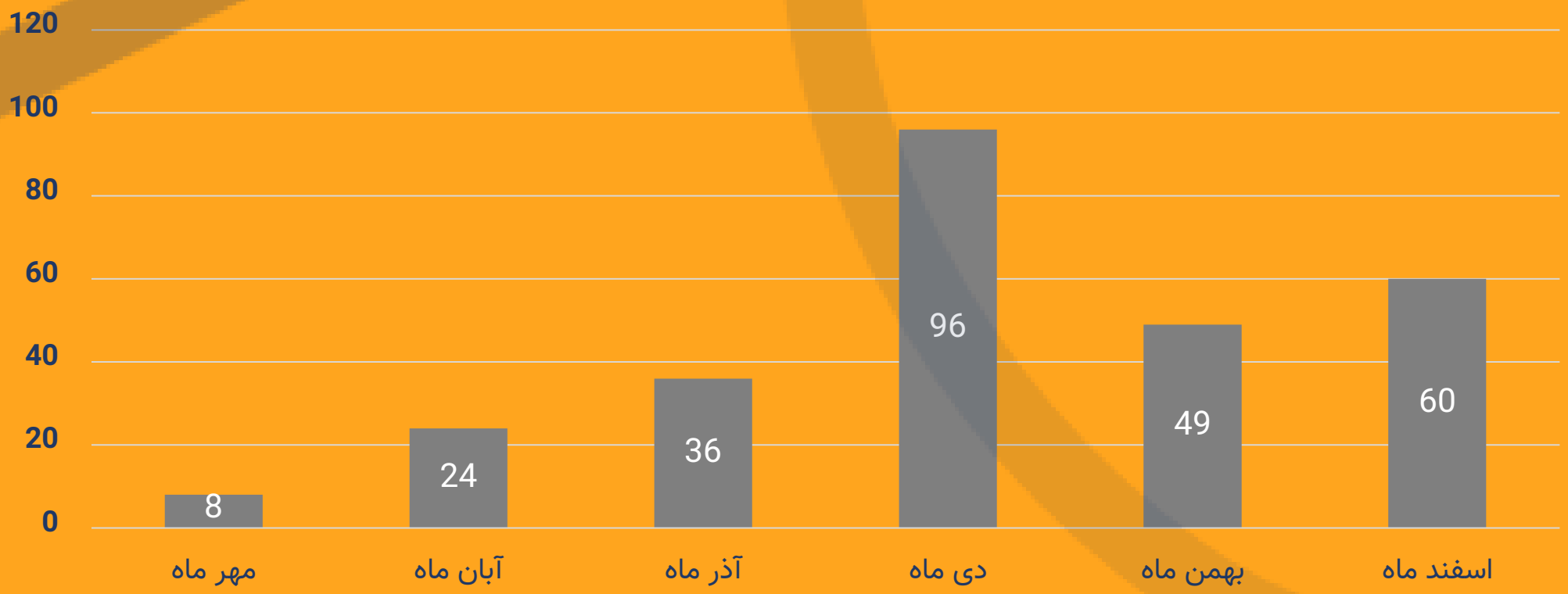
باگ بانتی در ایران

باگدشت به عنوان باگ بانتی ایرانی چه عملکردی داشته است؟

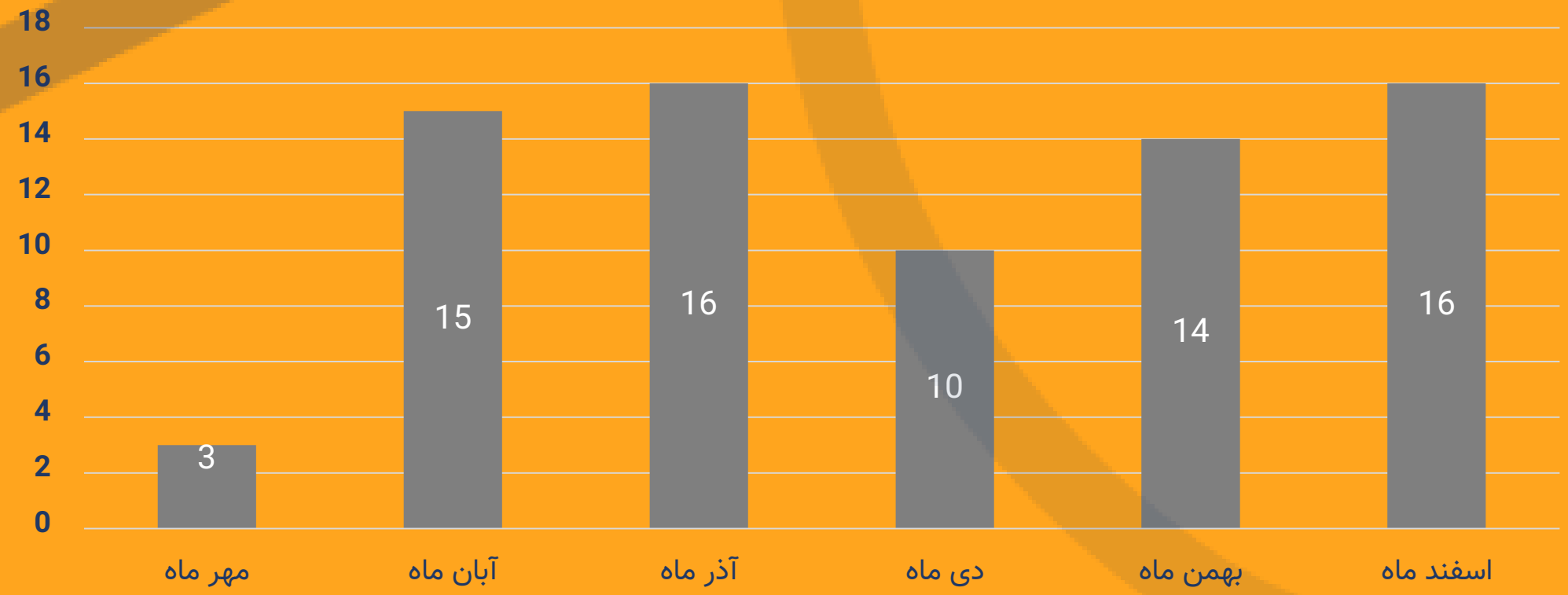
رشد تعداد متخصصین امنیتی در باگدشت



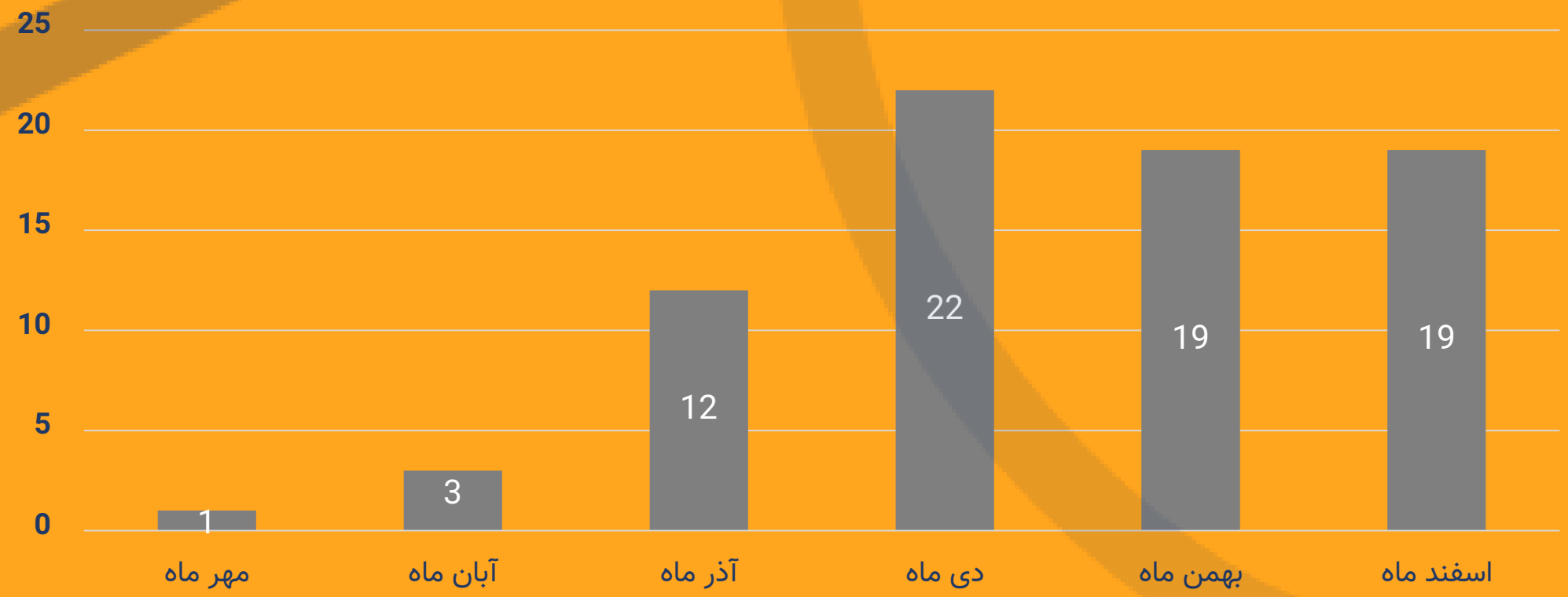
باگ های امنیتی شناسایی شده در باگدشت



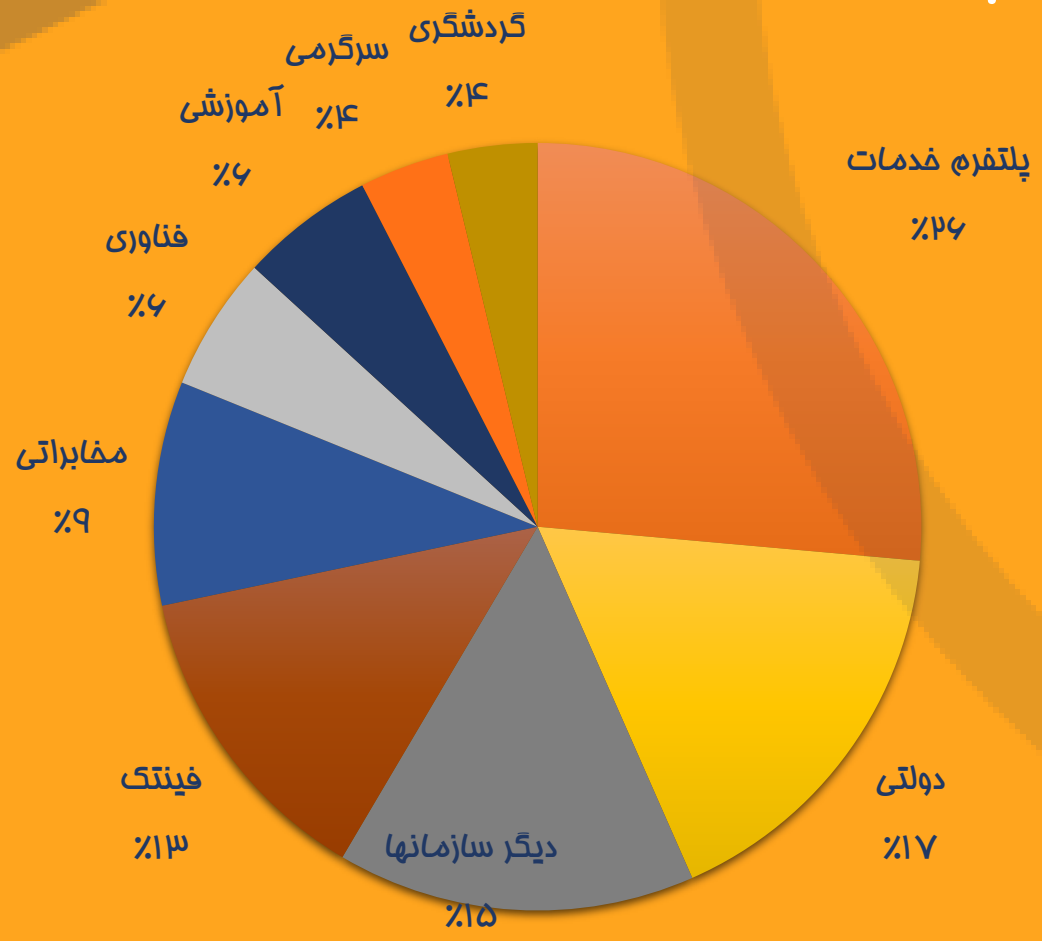
پرداختهای انجام شده به متخصصین باگدشت (میلیون تومان)



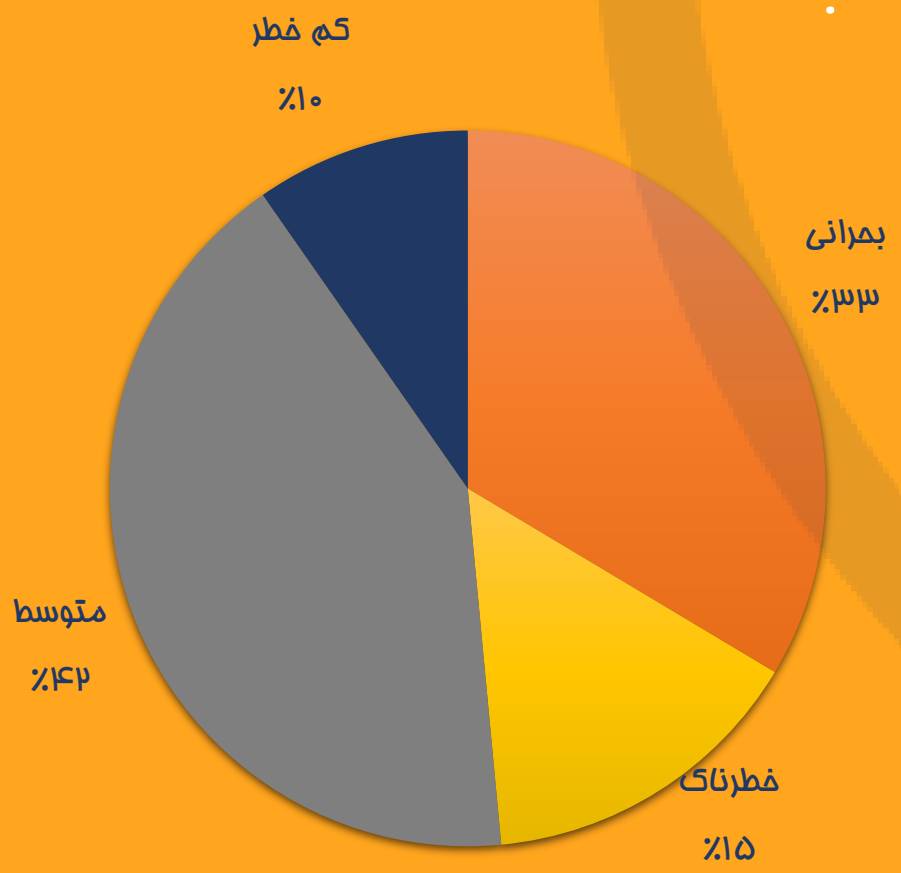
مقالات منتشر شده توسط باگدشت



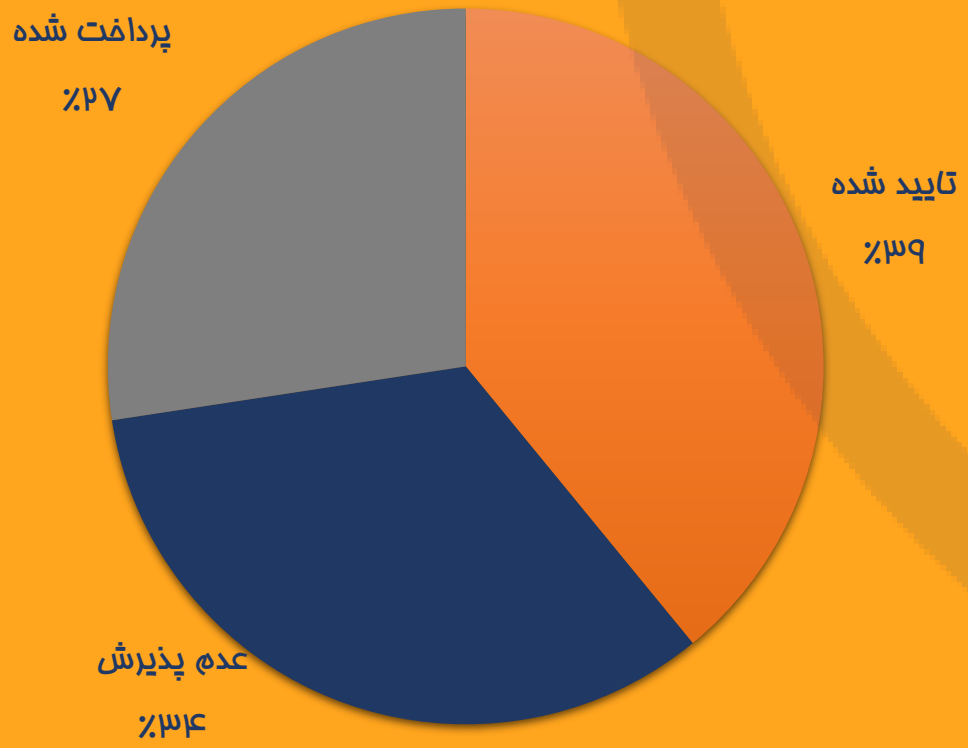
باگ های شناسایی شده توسط باگدشت به تفکیک صنایع



باگ های شناسایی شده توسط باگدشت به تفکیک شدت اهمیت



باگ های شناسایی شده توسط باگدشت
به تفکیک وضعیت



برترین متخصصین امنیت باگدشت در سال ۱۳۹۷

Hoseinroot	Davar	Hosseinro0t	UnderSc0rPi0n	Hojat
Rouzbeh	Evilroot	Mtoreihi	C3po	Thisismohammad
Choghook	Mnodhe	Looseking	MhmH	Mrpro
PooriaSnipe	Captain_Hook	AAtest	Tirex	Dmitriy_area51

چالشها و موفقیت های باگدشت در سال گذشته

- جذب حمایت و اعتماد متخصصین امنیت در کشور (متوسط 7 متخصص در هفته)
- و در نتیجه دریافت گزارشات باگ های امنیتی سامانه ها بصورت مستمر (متوسط 10 باگ در هفته)
- نیاز به اعتمادسازی سازمانها و همکاری مستمر با متخصصین امنیتی متعهد و مورد تایید با تخصص حرفه ای و ایجاد تیم VIP جهت بانتی های اختصاصی سازمانی
- برگزاری جلسات هم اندیشی و اعتماد سازی با مدیران فنی و امنیت سازمانها در خصوص چگونگی بهره برداری بهتر از باگ بانتی در کشور (متوسط 3 جلسه در هفته)
- برگزاری جلسات تخصصی با نهادهای قانونگذار، نظارتی، حقوقی و قضایی به منظور حمایت از ایجاد بستر قانونی باگ بانتی در کشور (متوسط 2 جلسه در ماه)
- تمرکز بر توسعه اکوسیستم باگ بانتی بصورت قانونی و دریافت مجوزهای "شورای عالی انفورماتیک کشور"، "سازمان نظام صنفی رایانه ای کشور"، "نماد اعتماد الکترونیکی" و "مرکز افتای ریاست جمهوری ایران"
- وجود ابهام و خلاهای قانونی و توسعه و شخصی سازی "سند اعلام آسیب پذیری" برای سازمانها و کسب و کارها (سند VDP یا Vulnerability Disclosure Program)
- تحلیل و رویایی با حواشی مختلف حرفه ای، اقتصادی و کسب و کار و ایجاد تیمی متخصص، متعهد و کارآزموده

مسیر باگ بانتی در باگدشت

خدمات امنیتی باگدشت

سطوح خدمات امنیتی باگدشت

در سطح پایه، باگ‌های تایید شده سطح Critical و High و Medium و LOW انجام می شود.

در سطح استاندارد، باگ‌های تایید شده سطح Critical و High و Medium و Low و راهکارهای ایمن سازی انجام می‌شود.

در سطح حرفه ای، باگ‌های تایید شده سطح Critical و High و Medium و Low و راهکارهای ایمن سازی و تست مجدد باگ و مشاوره ایمن سازی انجام می شود.

در سطح اختصاصی، ایجاد بانتی VIP از متخصصین مورد تایید و شناخته شده باگدشت از نظر تخصص و تعهد، دوره‌های تخصصی شخصی سازی شده در حوزه کدنویسی امن و ایمن سازی و ایمن سازی و هاردنینگ سامانه های سازمانی انجام می شود.

" تجربه من با باگدشت یه تجربه خوب و بی دردسر بود، البته همین هم انتظار داشتم، قبلا برای اینکه بتونم یه هکر پیدا کنم که باگ امنیتی سیستم رو پیدا کنه خیلی تلاش کردم اما در نهایت نتوستم به کسی اعتماد کنم اما اینجا چون باگدشت تضمین میده که سیستم آسیب نبینه و از باگ هاش سو استفاده نشه خیالم راحت بود. "

بهرام مشرفی، مدیرعامل دیتاشهر و یوتوپین

" استرس خطرات امنیتی یک وب‌سایت یا خدمت بر روی اینترنت همیشه می‌تونه یه خواب شب راحت رو از من بگیره. سپردن تست امنیتی وندار به باگدشت هم همین میزان استرس رو برای من ایجاد کرد، اما نتیجه باعث شد که شبهای بعدش رو راحت بخوابم. "

مهدی عبادی، مدیرعامل وندار

" باگدشت دریچه ای نو و استارتاپی متفاوت در امنیت سایبری کشور است. "

Thisismohammad

" باگ بانتی دوتا تا نکته جالب داره، اول اینکه تخصصی رو به تیم فنی وارد میکنه که از قبل وجود نداشته و متخصصان امنیت هم بصورت سازمان یافته فعالیت و درآمدزایی میکنند باگدشت به عنوان اولین پلتفرمی که این سرویس رو ارائه میده، تونسته این مدل رو به خوبی اجرا کنه و ما از خدماتی که از باگدشت دریافت کردیم راضی هستیم. "

صادق اشرفی، مدیر پروژه الوبیزنس

" اگه سازمان هستید می تونید با باگدشت حجم نامحدودی از هوش و خلاقیت هکرهای حرفه ای رو در جهت منافع سازمانتون دشت کنید و اگه هکری با جسارت هستید که دنبال منافع مالی و اعتبار بخشی و رزومه سازی برای خلاقیت هکری خودتون هستید اونو در میدون رقابتی حرفه ای و دوستانه با هکرهای دیگه در باگدشت، دشت کنید. "

محمد قیصری، مدیرعامل مرکز تحقیقات اینترنت اشیا

" باگدشت یک ایده خلاقانه با ظرفیت هایی فوق العاده و حرفه ای است . "

Hoseinroot


همکاران سیستم
SYSTEM GROUP

الوبیزنس


شرکت بهسازان ملت
بانکداری نوین


نت برگ
Netbarg


همراه کارت


Pelak


وندار


Bitbarg


دای کِهِ
DAYCHE
گروه داده کاوی دایکه

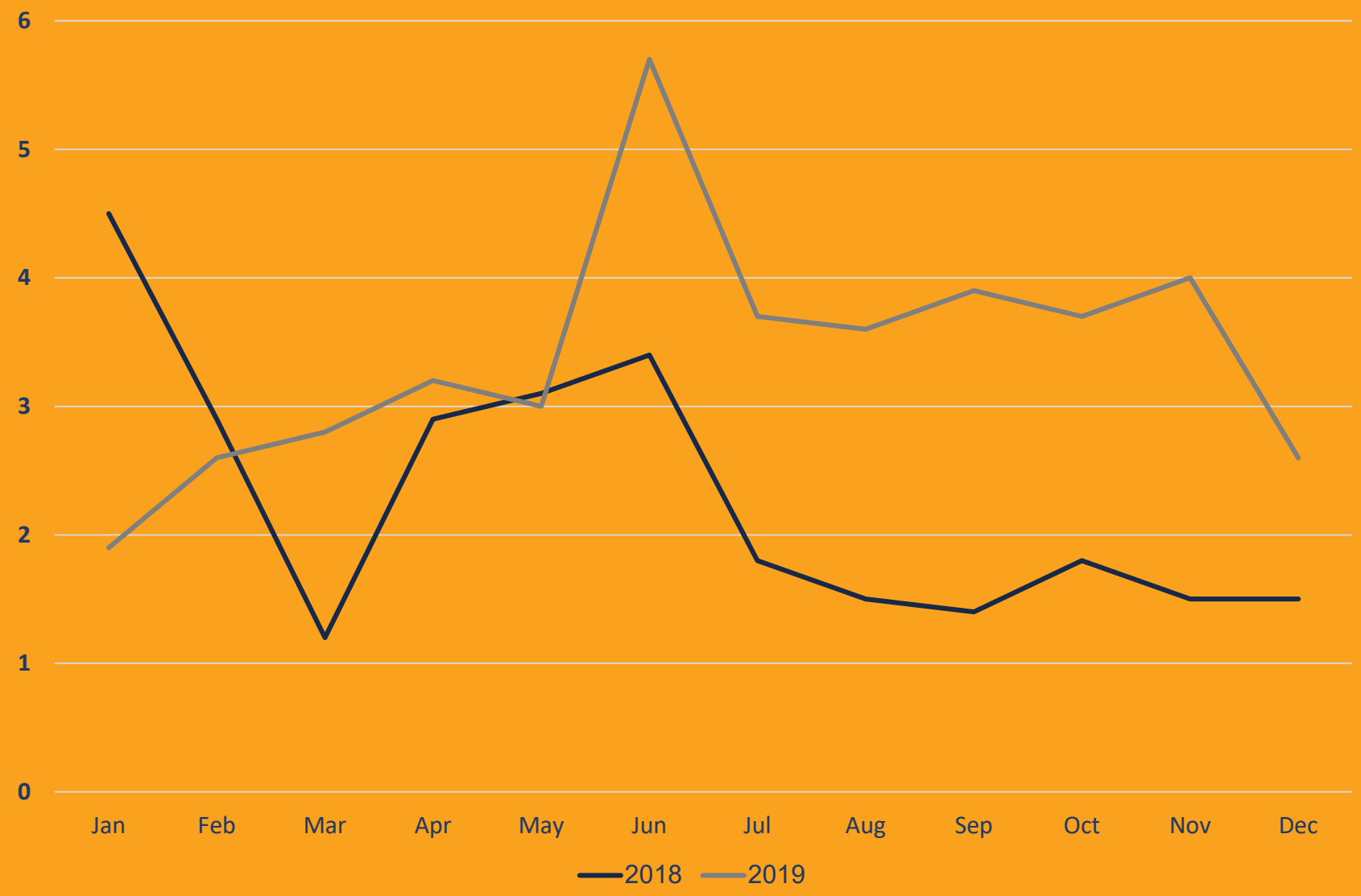

شرکت خدمات انفورماتیک
informatics services corporation

آیا شما هم به عنوان مدیر فنی یا مدیر امنیت سازمان، با این مشکلات و چالش ها در پروژه های ارزیابی امنیتی برخورد داشته اید؟

آیا اطلاعات آمارهای جهانی برای سازمان شما هم معنادار است؟


افشای اطلاعات Quora در سال ۲۰۱۸ با ۱۰۰ میلیون رکورد
دسترسی غیرمجاز به برنامه visual studio در سال ۲۰۱۹
افشای اطلاعات Instagram و Facebook در سال ۲۰۱۹ با ۵۰۰ میلیون
BUGDASHT NEWS
افشای اطلاعات FEMA در سال ۲۰۱۹ با ۲ میلیون رکورد (دولتی–نظامی)
دسترسی غیرمجاز در Adobe در سال ۲۰۱۹ با ۷ میلیون رکورد
افشای اطلاعات Facebook در سال ۲۰۱۸ با ۵۰ میلیون رکورد
افشای اطلاعات T-Mobile در سال ۲۰۱۸ با ۲ میلیون رکورد
افشای اطلاعات Orvibo در سال ۲۰۱۹ با ۱ میلیون رکورد (IoT)
افشای اطلاعات British Airways در سال ۲۰۱۸ با ۳۸۰ هزار رکورد
دسترسی غیرمجاز به اپ واتساپ و iPhone در سال ۲۰۱۹
افشای اطلاعات First American در سال ۲۰۱۹ با ۸۸۵ میلیون رکورد (بانکی)

حملات برنامه های مبتنی بر وب (میلیون)

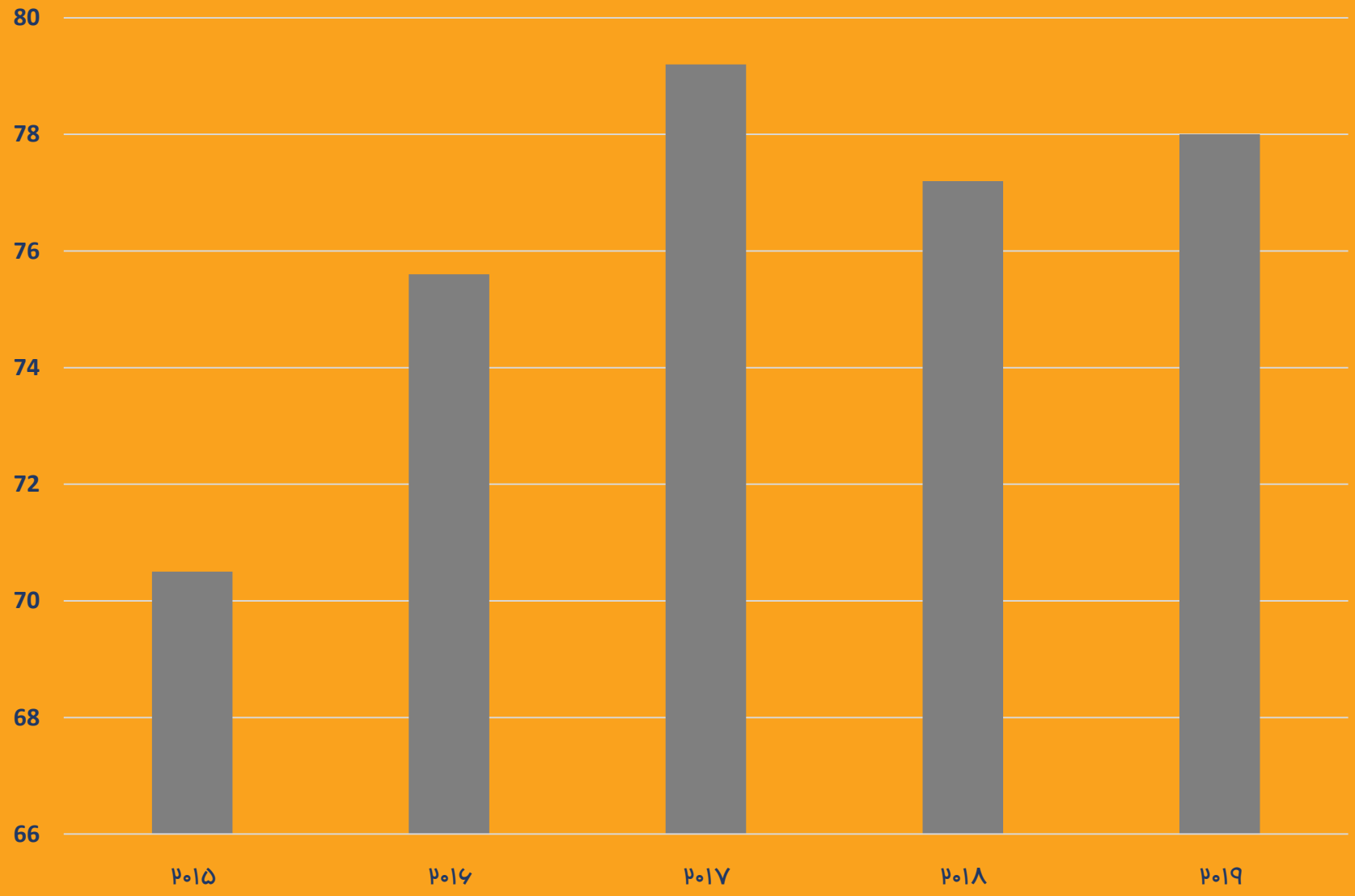


با توسعه خدمات و سامانه های کسب و کارها مبتنی بر فضای وب، میزان آسیب پذیری آنها و در نتیجه دسترسی های غیرمجاز و سواستفاده از مشکلات امنیتی افزایش یافته است.

مهاجمین با اهداف مختلف از جمله دسترسی به اطلاعات مشتریان، سواستفاده از داده های سازمانی و یا حتی بهره برداری در حملات دولتی و هدفمند سامانه های وب را که بیشترین مشکلات امنیتی را دارا می باشند مورد هدف قرار می دهند و با تجمیع اطلاعات بدست آمده،اهداف خود را اجرا می نمایند.

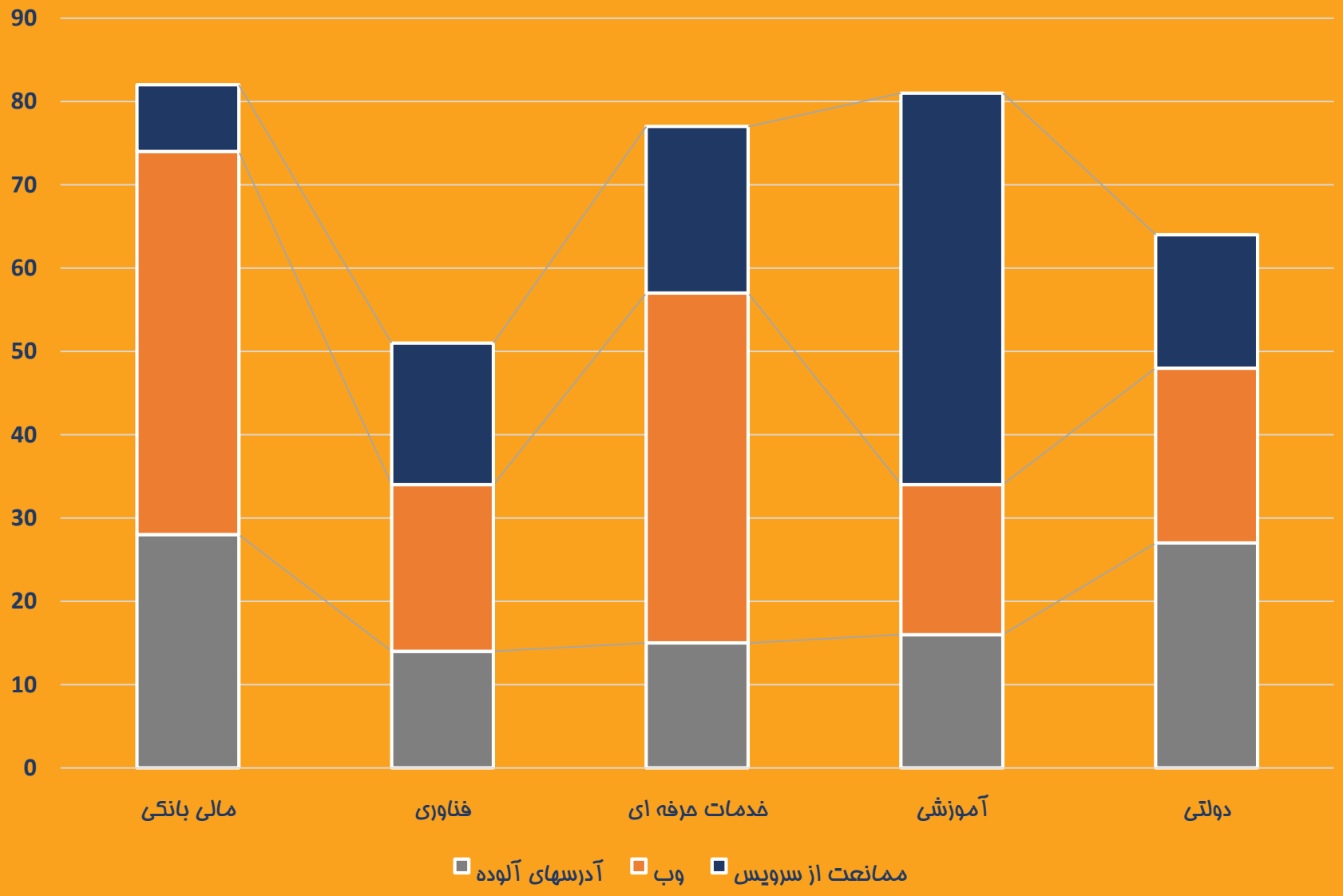
در سالهای اخیر، کسب و کارهای کوچک و متوسط نیز در رشد حملات مهاجمین قرار گرفته اند، زیرا محل مناسبی برای ذخیره سازی و دسترسی غیرمجاز به اطلاعات مشتریان هستند.

درصد حملات موفق در سال



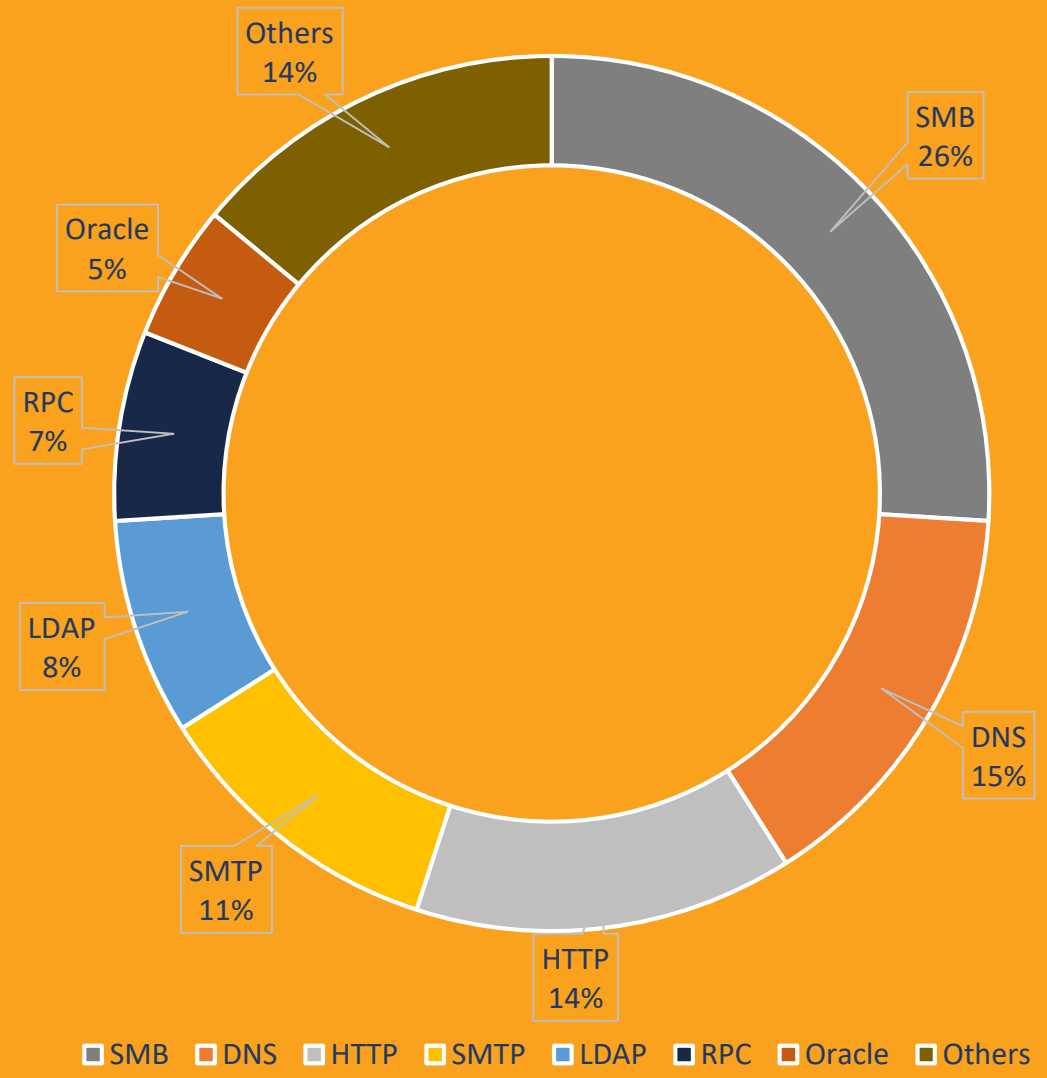
با توجه به تغییرات متنوع و مختلف بر اساس نیازمندیهای کسب و کارها در سامانه ها و توجه کمتر به ملاحظات امنیتی و ایمنی حریم خصوصی مشتریان، روز به روز بر تعداد آسیب پذیری های امنیتی سامانه ها افزوده می شود.
از سوی دیگر با توسعه سامانه ها بدون در نظر گرفتن خط مشی های امنیتی در هنگام تولید محصول، پیگیری و به روزرسانی ویژگی های محصولات به سختی صورت می گیرد.
این فضا بستر مناسبی را برای مهاجمین جهت اجرای موفق حملات خود و دسترسی به اطلاعات مورد نیاز را با کمتریم تلاش برای آنها فراهم آورده است.

انواع حملات شناسایی شده و نوع آنها به تفکیک صنعت



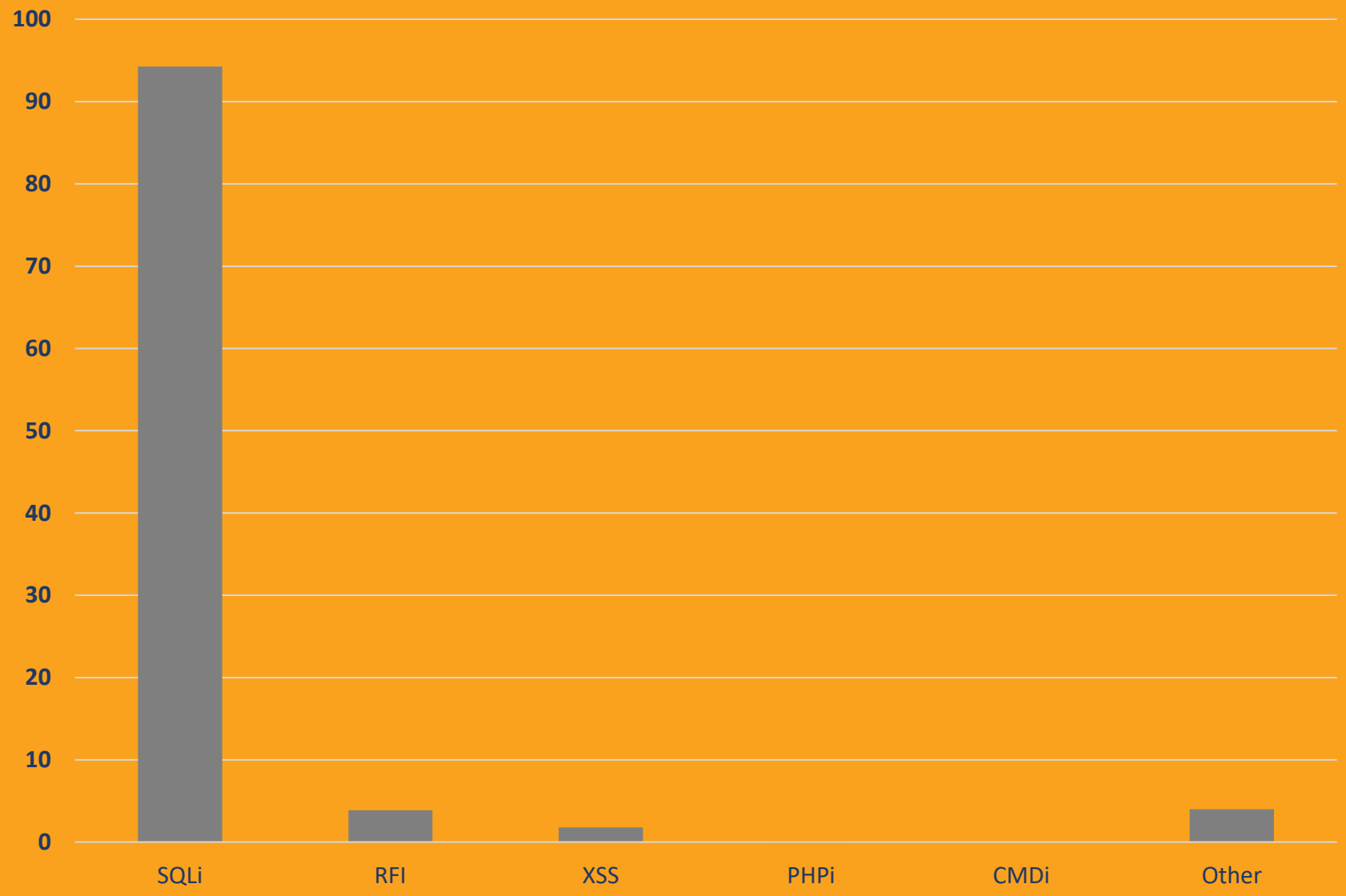
حملات مبتنی بر وب صدر حملات شناسایی شده و انجام شده در سالهای اخیر در صنایع مختلف را دارا می باشند.
اهداف تغییر و دسترسی به اطلاعات محرمانه از مهمترین دلایل اجرای حملات مبتنی بر وب می باشد.
بر اساس گزارش IBM، موسسات مالی و بانکی و فینتک ها در سه سال پیاپی اصلی ترین هدف مهاجمین بوده اند.
آلوده سازی نودها و تجهیزات سازمانی و همچنین اجرای حملات منع سرویس از اولویت های بعدی در صنایع با اطلاعات حساس می باشد.

سرویسهای مورد استفاده در حملات



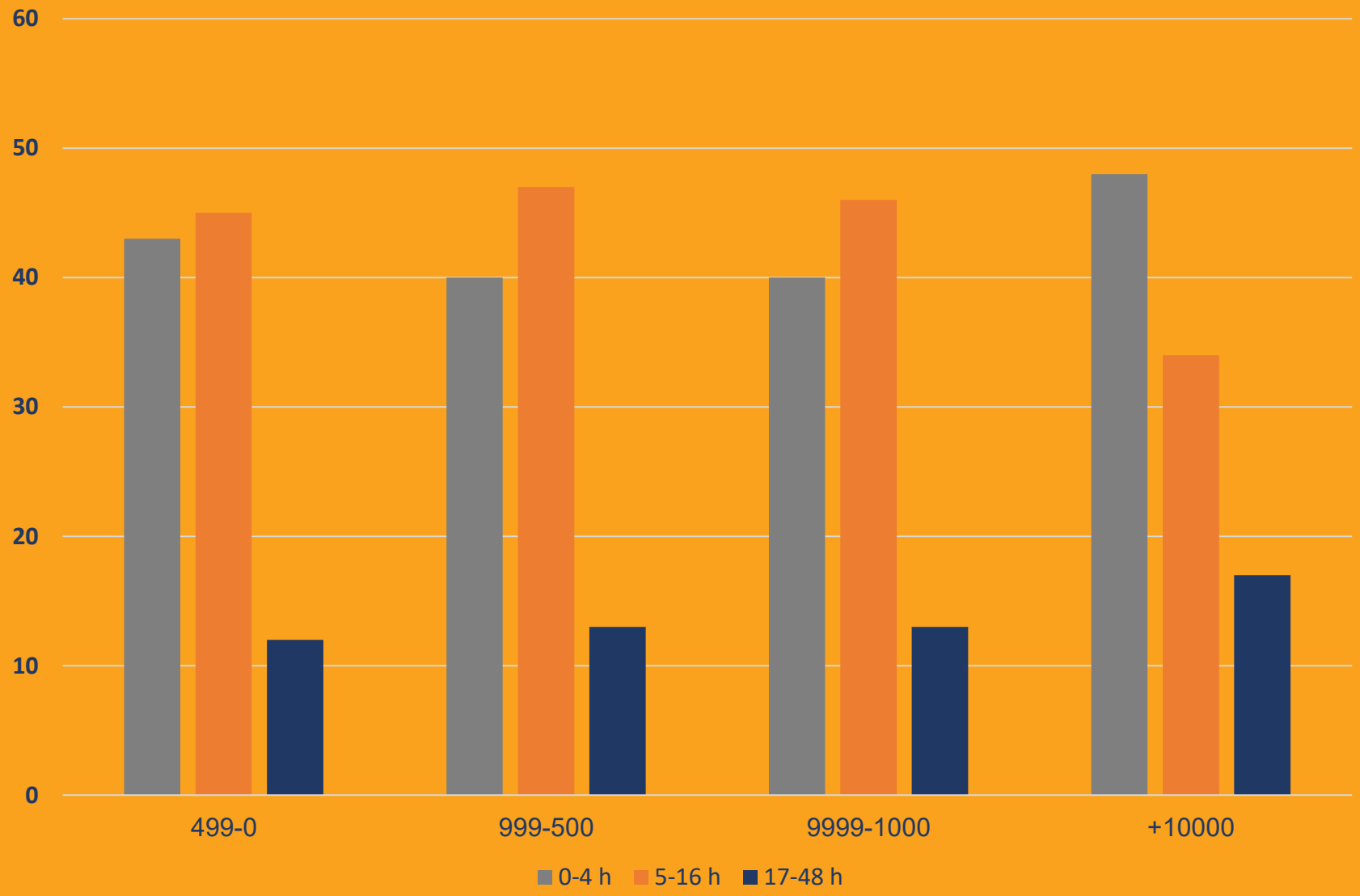
علیرغم آسیب پذیری های شناسایی شده در سالهای اخیر در خصوص سرویس های پرکاربرد در سازمانها، بسیاری از کسب و کارها به به روزرسانی و ایمن سازی سامانه ها و دارایی های اطلاعاتی خود بی اهمیت می باشند.
همچنان در سازمانها فرآیندهای مدیریت وصله و بررسی به روز آسیب پذیری های امنیتی و مطابقت آنها با دارایی های سازمانی وجود ندارد که طبیعتا مهاجمین نیز از این موضوع آگاه هستند و از همین نقاط ضعف، دسترسی های مورد نیاز خود را ایجاد می نمایند.
بر اساس گزارش Gartner، در سال 2020 اکثر رخدادهای امنیتی از آسیب پذیری های شناسایی شده و اعلام شده به سازمانها به وقوع می پیوندد.

درصد بردار حملات برنامه های کاربردی (۲۰۱۷ تا ۲۰۱۹)



همچنان وقوع رخدادهای امنیتی به دلیل عدم رعایت ضوابط کدنویسی ایمن از بزرگترین مشکلات در سال گذشته بوده است.
عدم صحت سنجی صحیح ورودی های کاربر، ذخیره سازی نا ایمن و پیاده سازی بر اساس تنظیمات پیش فرض و در نتیجه انتقال مسوولیت امنیت سامانه به تکنولوژی مورد استفاده بدون در نظر گرفتن راهنماهایی ایمن سازی، منجربه اجرای حملات مبتنی بر وب و دسترسی به اطلاعات محرمانه سازمانها در سال 2019 شده است.

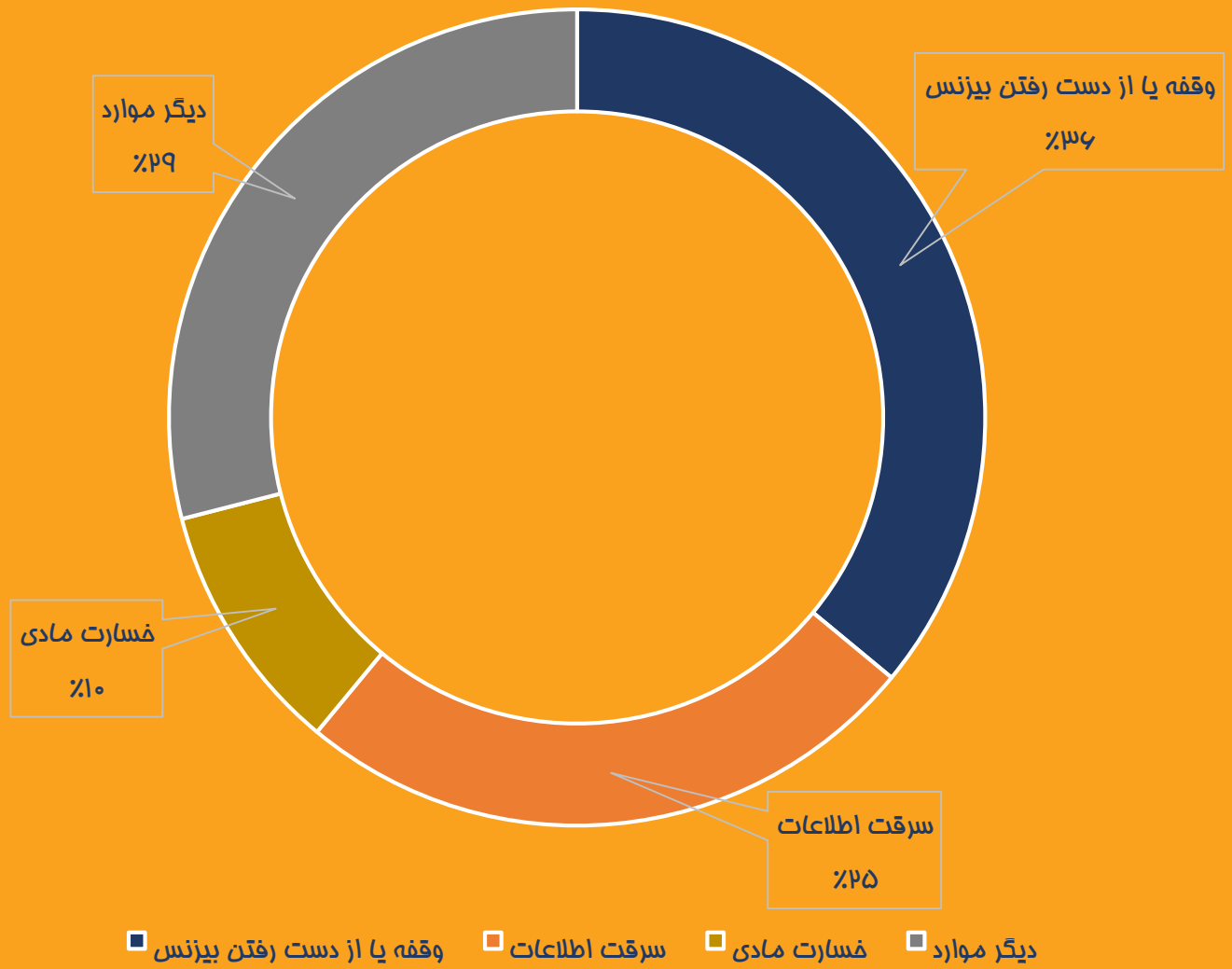
میزان ساعات از دست رفتن سرویس سازمانها در زمان رخداد



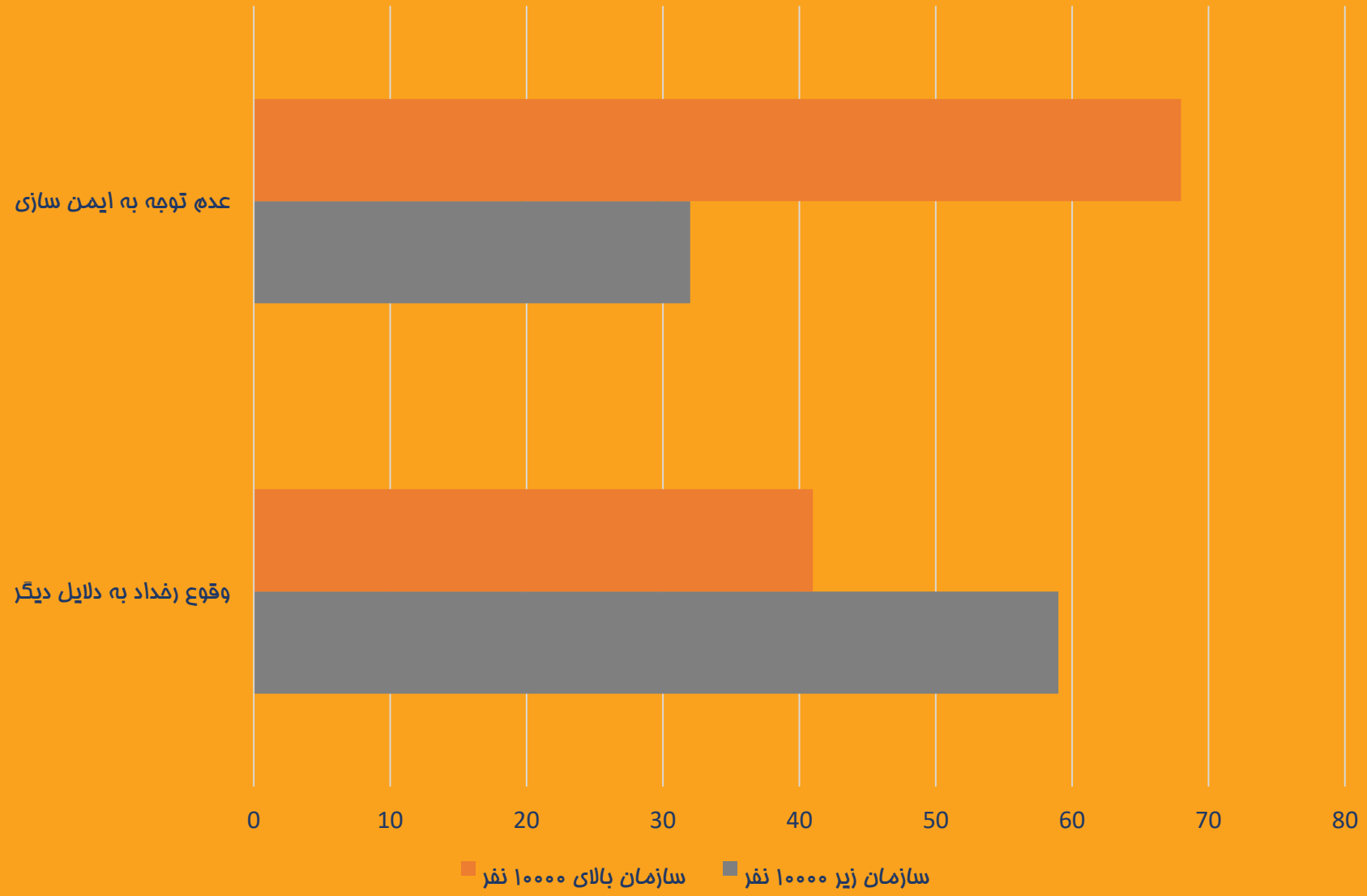
رقابت بیشتر در ارایه خدمات مبتنی بر فضای وب به مشتریان از یک سو و همچنین تایید نهادهای نظارتی و رگولاتوری دو رکن اساسی در پیشگیری از وقوع رخدادهای امنیتی در سازمان می باشد.
وجود بلوغ سازمانی در توسعه فرآیند شفاف در هنگام وقوع رخدادهای امنیتی، تعیین مسوولیت سازمان در قبال اطلاعات مشتریان، دسترسی به کارشناسان متخصص و آموزش دیده برای بازیابی صحیح سرویس های مورد هدف قرار گرفته و همچنین پشتیبانی مدیران ارشد سازمانها در سرمایه گذاری در زمینه امنیت سازمان به عنوان راهکاری پیشگیرانه از مهمترین چالش های این بخش است.

پیامدهای رخداد امنیتی بر سازمانها

با وقوع رخدادهای امنیتی در خصوص سامانه های سازمانی پیامدهای متفاوتی قابل اجرا می باشد.
از دسترسی و افشا اطلاعات مشتریان سازمان تا از دست رفتن سرویسهای کسب و کار و عدم امکان ارایه خدمات به مشتریان سازمان یا وقوع خسارتهای مادی بزرگ به سازمان که می تواند چالش جدی در فضای رقابتی برای سازمان باشد.
از دیگر پیامدهای وقوع رخدادهای امنیتی در سازمانها می توان به لغو مجوزهای فعالیتی از سوی نهادهای رگولاتوری، عدم دسترسی به اهداف بیزنس و پیشی گرفتن رقبا و یا درگیر شدن سازمان با مسایل حقوقی و قضایی اشاره نمود، که همگی سازمان را از تمرکز بر اهداف اصلی خود باز می دارد.

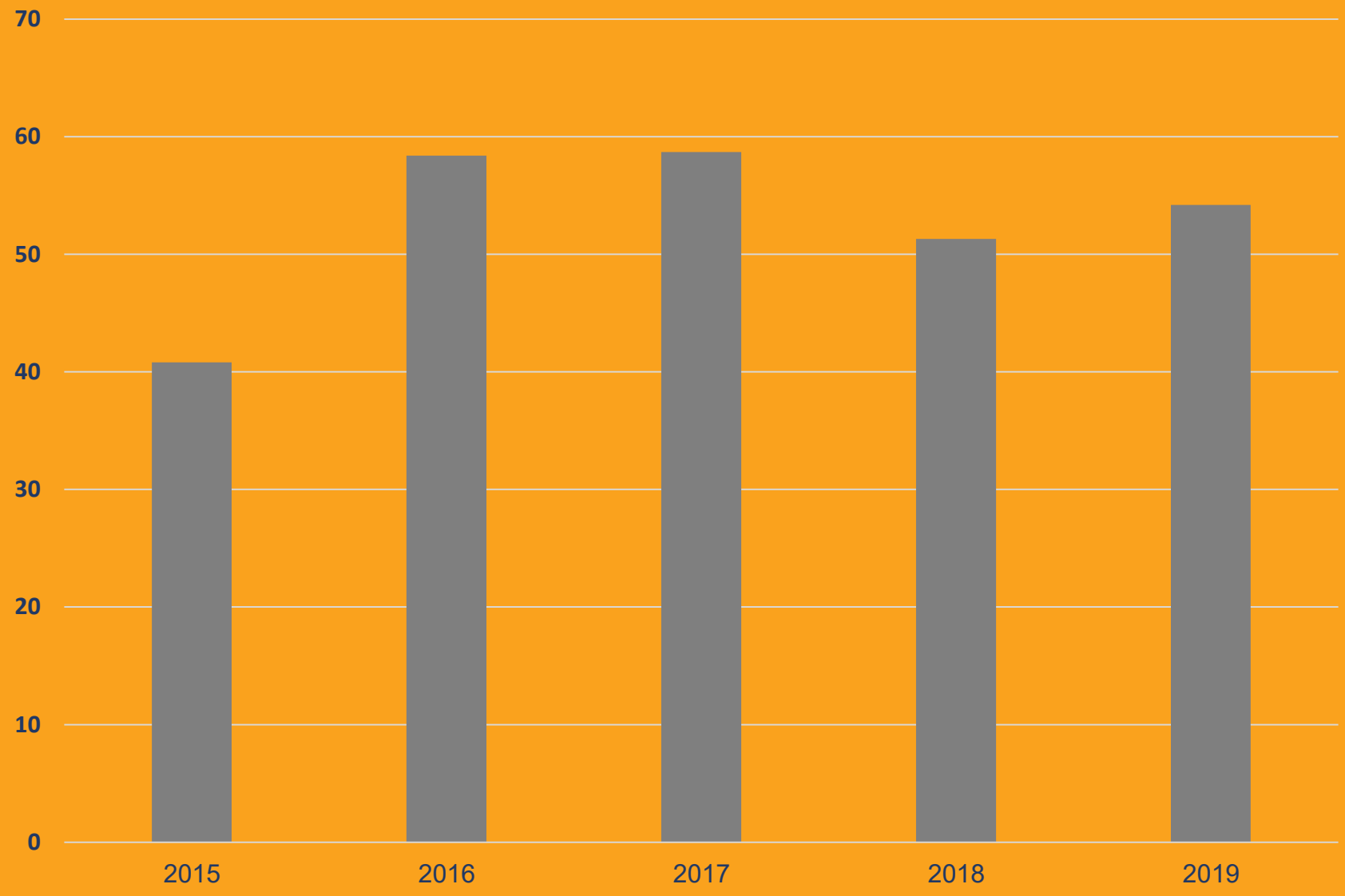


دلایل وقوع رخداد امنیتی



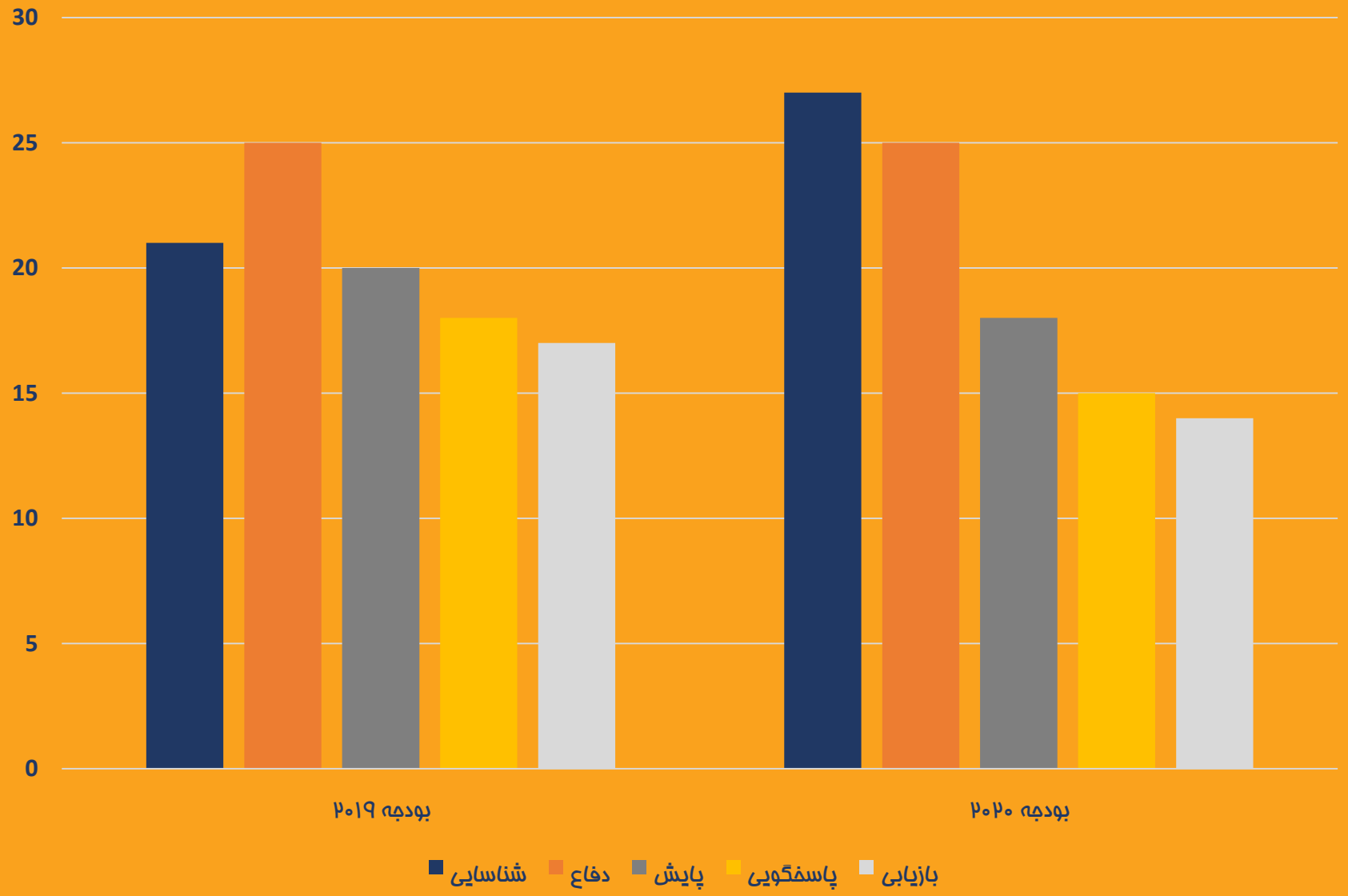
بر اساس گزارش cisco مهمترین نگرانی وقوع رخدادهای امنیتی در سال 2020، عدم توجه کافی به چرخه مدیریت وصله های امنیتی در سازمان می باشد.
سازمانهایی که رخداد امنیتی خود را به دلیل نبود توجه به ایمن سازی سامانه های خود در سال گذشته تجربه کرده اند، میزان افشای اطلاعات بیشتر و حیاتی تری را گذرانده اند. 68 درصد سازمانهایی که ایمن سازی مناسبی را در سازمان پیاده سازی ننموده اند، بیش از 10.000 رکورد را از دست داده اند.
ایمن سازی امری پیچیده و نیازمند تخصص برای عدم تداخل در فرآیند اصلی کسب و کار است ولی پیاده سازی آن می تواند نرخ بازگشت سرمایه در کسب و کار را به شدت افزایش دهد.

سازمانهایی که بیش از ۱۰ درصد از بودجه خود را صرف امنیت می نمایند



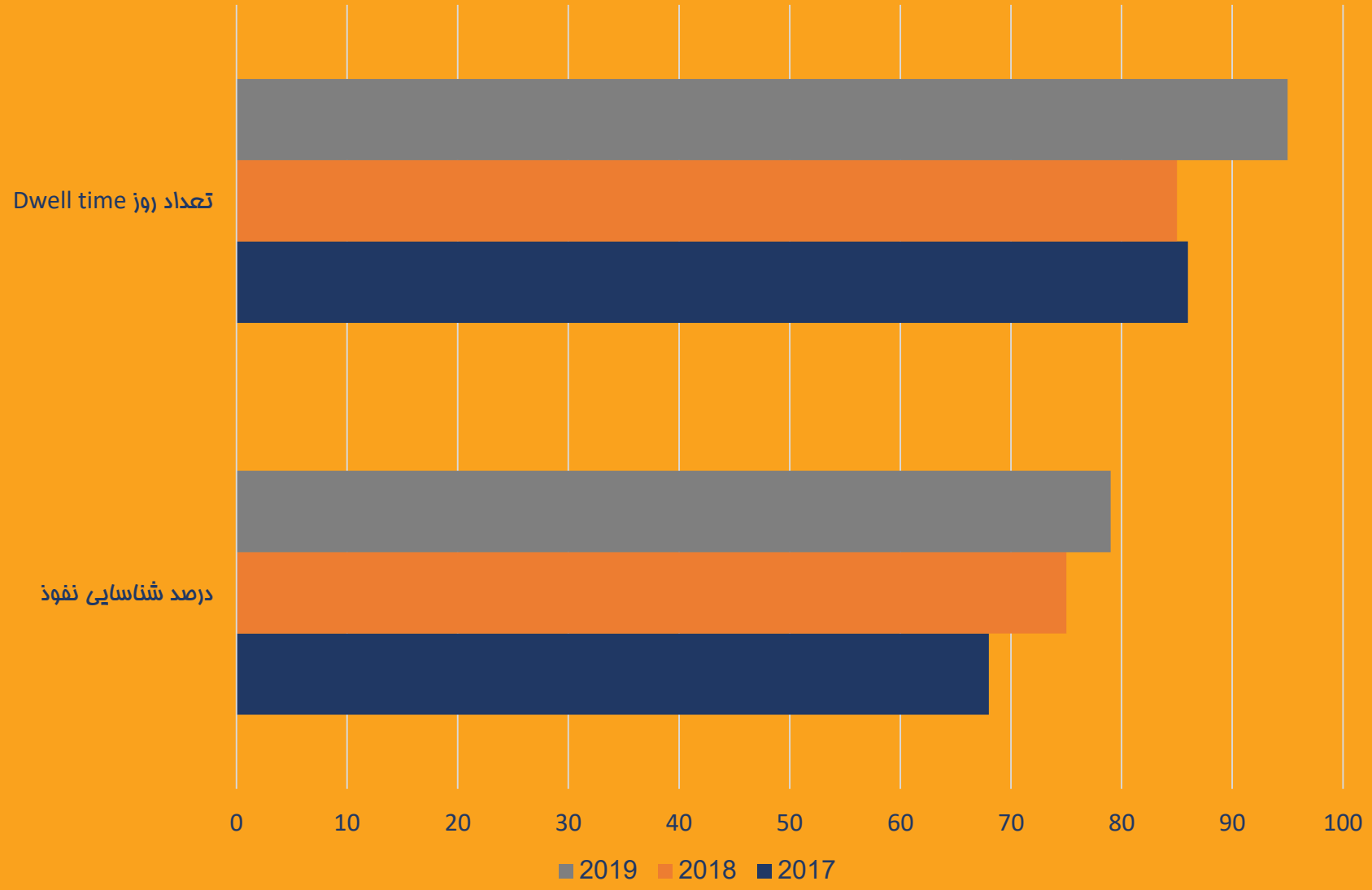
در گزارش سالانه CDR، سازمانهایی که در طول پنج سال گذشته بیش از 10 درصد از بودجه فناوری اطلاعات خود را در زمینه امنیت سایبری تخصیص داده اند بررسی شده اند.
بیشترین میزان تخصیص بودجه به امنیت سایبری در سازمانهای بزرگ می باشد و این میزان در هر صنعت کمتر از 12 درصد نبوده است.
این بودجه در زمینه شناسایی مشکلات امنیتی، آموزش پرسنل، خودکارسازی فرآیندها و راهکارهای پاسخگویی به رخدادهای امنیتی بوده است.
افزایس میزان بودجه امنیت سایبری به ترتیب در صنایع پزشکی، مخابراتی، کارخانجات، مالی، دولتی، خرده فروشی و آموزشی بوده است.

بودجه سازمانها در مدیریت رخدادهای امنیتی



سازمانها در سال گذشته بر اساس تخصیص بودجه خود در چرخه حیات دفاع سایبری و مدیریت رخداد مورد بررسی قرار گرفته اند.
Cisco اعلام نموده است که تمرکز سازمانها به نسبت سال گذشته از موارد تدافعی در برابر رخدادهای امنیتی به آیتمها و راهکارهای پیشگیرانه منتقل شده است.
علیرغم افزایش بودجه تخصیص داده شده به امنیت سایبری، سهم هر بخش تغییر یافته است. دفاع و پایش رخدادهای امنیتی تقریبا میزان مشابه سال گذشته خود را داشته اند و در مقابل پروژه هایی که منجربه شناسایی منابع جدید برای امنیت سازمانها گردد و سهم بازیابی سامانه و پاسخگویی در مقایسه با سال گذشته کاهش داشته است.

عملکرد سازمانها در شناسایی نفوذ



در گزارش Symantec نرخ سازمانهایی که قادر به شناسایی نفوذ موفق به دارایی های اطلاعاتی خود را داشته اند، افزایش یافته است. این عدد در سال 2019 به میزان 79 درصد بوده است.
همچنان مشاهده می شود سازمانها بسیاری از نفوذهای صورت گرفته به سازمان خود را شناسایی نمی نمایند.
در این گزارش زمان میان وقوع نفوذ به سازمان تا زمان شناسایی آن را مورد بررسی قرار داده اند که همچنان بازه قابل توجهی را در بر دارد.
سازمانهای نیازمند منابعی هستند تا بتوانند سریعتر مشکلات امنیتی خود را متوجه شوند و سریعا آنها را ایمن سازی نمایند تا حتی با وجود دسترسی انجام شده از گسترش آنها جلوگیری شود.

راهکار ارتقا امنیت سامانه ها در سازمان با وجود مشکلات چیست؟

به چه روشی امنیت در چرخه حیات سامانه های سازمان یکپارچه می شود؟

افزایش منابع همزمان در هریک از فازهای چرخه حیات توسعه محصول با تمرکز بر فاز شناسایی

تحلیل استاتیک کد

تحلیل استاتیک کد معمولا نخستین روش برای ارزیابی امنیتی نرم افزارها بصورت جعبه سفید با دسترسی کامل به کد منبع می باشد و دارای قدمت بسیاری است و درصورتیکه با ابزار و دانش امنیتی تخصصی صورت گیرد دارای نتیجه و اثربخشی خوبی می باشد. آسیب پذیری هایی که معمولا در این روش شناسایی می گردند شامل مشکلات شناخته شده امنیتی از دیدگاه توسعه دهنده مانند سرریزبافر یا انواع حملات تزریق می شود. به دلیل حجم بالای کدهای سازمانی، تحلیل کدها بصورت دستی برای تیم توسعه دهده و یا امنیت قابل انجام نیست و معمولا از ابزارهای تحلیل کد برای این منظور استفاده می شود.

تست نفوذ

تست نفوذ یا پنتست، شبیه سازی حملات مختلف در مقابل سامانه و یا زیرساخت پیاده سازی نرم افزار می باشد تا بتواند نقاط دارای ضعف امنیتی شناسایی گردد. تست نفوذ به زیرشاخه های متفاوتی تقسیم می شود. برخی از آنها بر روی ارتباطات و مشکلات پیاده سازی و پیکربندی عناصر شبکه ای تمرکز دارند، برخی بر روی باگ های امنیتی نرم افزاری. سازمان در پروژه های تست نفوذ می بایست هزینه پروژه را بر اساس نفر ساعت پیمانکار و اجرای تست پرداخت نماید. هزینه های مربوط به کارشناس متخصص، تیم اجرایی سازمان و استفاده از ابزارهای امنیتی و لایسنس آنها نیز به آن افروده می شود. تست نفوذ در شرایط و محیط تست اجرا می شود و کمتر در محیط های اجرایی و تجاری سازی شده پیاده سازی می گردد.

ارزیابی انطباق

ارزیابی انطباق برای بررسی میزان انطباق پیکربندی، معماری و فرآیندهای مشخص شده سازمانی با قوانین بالادستی و یا استانداردهای امنیتی می باشد. این ارزیابی تنها به بررسی های امنیتی محدود نمی شود و می تواند شامل حداقل های مورد پذیرش در عملکرد و زمان پاسخدهی نیز باشد. اگرچه اگر این ارزیابی را به موارد امنیتی محدود کنیم می تواند شاخص برآورده سازی حداقلهای رعایت شده توسط سازمان در خصوص آن سامانه باشد.

ارزیابی آسیب پذیری

ارزیابی آسیب پذیری بسیاری از مواقع با مفهوم تست نفوذ اشتباه گرفته می شود. ارزیابی آسیب پذیری پروسه شناسایی خودکار و ابزار محور شناسایی آسیب پذیری های شناسایی شده در محصولات و یا سامانه های سازمان می باشد و معمولا به ارایه چک لیست های امنیتی محدود می شود که دارای نتایج مثبت کاذب بسیاری است و بهینه انجام نمی شود.

باگ بانتی

باگ بانتی، ارزیابی مستمر سامانه های سازمان است که به سازمان اجازه جلوگیری از حملات سایبری، سرقت داده و یا سواستفاده از آنها را می دهد. ارزیابی امنیتی توسط هکرهای اخلاقی که برای شناسایی آسیب پذیری های مرتبط با آن سرویس و یا برنامه های کاربردی پاداش دریافت می نمایند اجرا می شود. برنامه های باگ بانتی، دارای بعد زمانی بیشتری هستند. ویژگی باگ بانتی ایجاد رقابت میان اجتماع بزرگی از متخصصین امنیت است که برای دریافت جایزه تلاش می نمایند. فرآیندهای شفاف پذیرش باگ، مسایل حقوقی و تخصص در ارزشگذاری از جمله مفاهیم اصلی باگ بانتی ها هستند.

آیا باگ بانتی، تست نفوذ را نقض می نماید؟

- این تصور که تست نفوذ، باگ بانتی و ارزیابی امنیتی داخلی در مقابل هم قرار می گیرند اشتباه است. هیچ کدام از آنها به تنهایی نمی توانند تمامی آسیب پذیری های سیستم را شناسایی کنند. در واقع، قبل از اینکه یک سامانه تجاری سازی شود و یا پس از تغییرات اساسی در خدمات، پیشنهاد می شود که تست نفوذ دقیق صورت پذیرد.
- هنگامیکه سامانه به سطح تجاری سازی پایه رسید، آماده است که باگ بانتی آغاز گردد. باگ بانتی می تواند ویژگی های آنلاین سیستم را بررسی کند و سازمان میتواند تست محیط عملیاتی و محیط تست را انتخاب نماید.
- نکته ای که در باگ بانتی دارای اهمیت است، ارزیابی بصورت مستمر و درازمدت است. حداقل بازه زمانی باگ بانتی 3 تا 6 ماه می باشد که بازه های زمانی بیشتر ایده ال هستند. مسلما زمانهایی در این بازه زمانی بدون شناسایی باگ امنیتی می باشد که معمولا به دلیل انتخاب نادرست جوایز بر اساس پیچیدگی تست امنیتی می باشد.
- آسیب پذیری های دارای کیفیت در باگ بانتی مزایای بسیاری به سازمان در جهت شناسایی و تطبیق سریع چرخه عمر توسعه محصولات را می دهد و سازمان می تواند مشکل امنیتی گزارش شده را در دیگر سامانه ها و یا در توسعه های آتی خود در نظر بگیرد.
- تعداد زیادی از متخصصین امنیتی با مهارتهای مختلف نسبت به اجرای تست اقدام می نمایند. آنها می توانند آسیب پذیری های نادر که معمولا حتی در تست نفوذ مشاهده نمی شود را شناسایی نمایند.

تجربه دیگر کشورها در باگ بانتی چگونه است؟

مفهوم باگ بانتی از چه زمانی استفاده می شود؟

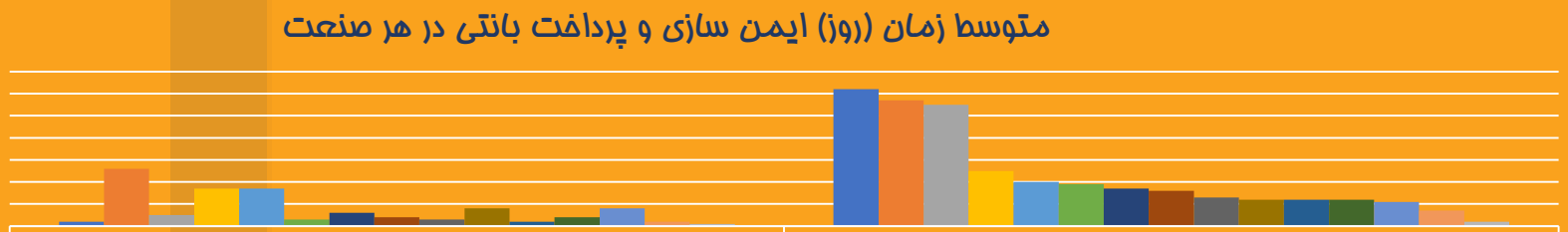
تاریخچه باگ بانتی

- اولین پرداخت باگ بانتی در سال 1851 به ازای باز نمودن یک قفل فیزیکی با ارزش معادل 200 شمش طلا صورت گرفت!!
- سال 1995، Netscape اولین باگ بانتی آنلاین برای Navigator 2.0 Beta را اجرا نمود.
- سال 2002، IDefense به عنوان واسط فنی پرداخت 400 دلار برای مشکلات امنیتی نرم افزارهای مختلف را در پلتفرم خود پیاده سازی نمود.
- سال 2004، باگ بانتی Mozilla و پرداخت حدود 500 دلار برای باگ های بحرانی صورت گرفت.
- سال 2005، TippingPointبه عنوان واسط فنی وارد باگ بانتی ها شد و آن را پلتفرم Zero Day Initiative یا ZDI نامگذاری نمود.
- سال 2007، در کنفرانس CanSecWest، مسابقات Pwn2Own اعلام شد و حدود 10.000 دلار برای سیستم عاملهای Mac پرداخت شد.
- سال 2010، مهمترین ترند در حوزه باگ بانتی های وب به وقوع پیوست و شرکت گوگل آن را آغاز نمود به همراهی شرکتهای دیگر مانند Mozilla، Baracuda و دو شرکت پستی فدرال آلمان و هلند.
- سال 2011، شرکت فیسبوک در همراهی با گوگل، پرداخت جوایز حداقل 500 دلاری را اجرا نمودند. (تاکنون بیش از 2 میلیون دلار پرداخت شده است)
- مجوعه BugCrowd پلتفرم واسط فنی باگ بانتی در امریکا، در سال 2011 برای ارایه خدمات واسط فنی و حقوقی ایجاد شد.
- سال 2013، Synack پلتفرم واسط فنی و حقوقی شناسایی باگ در نهادهای دولتی و نظامی امریکا شکل گرفت.
- مایکروسافت و فیسبوک بصورت همکاری مشترک حمایت از ایجاد باگ بانتی اینترنت (IBB) بصورت OpenSource و شناسایی باگ های فریم ورک ها مانند Ruby، Django را توسعه دادند.
- سال 2015، پلتفرم باگ بانتی HackerOne برای ارایه خدمات واسط فنی و حقوقی باگ بانتی ایجاد شد.
- و این روند به دلیل مزیت های ایجاد شده برای ایمنی سازمانها، همچنان ادامه دارد.

پلتفرم های بین المللی باگ یابی در دنیا

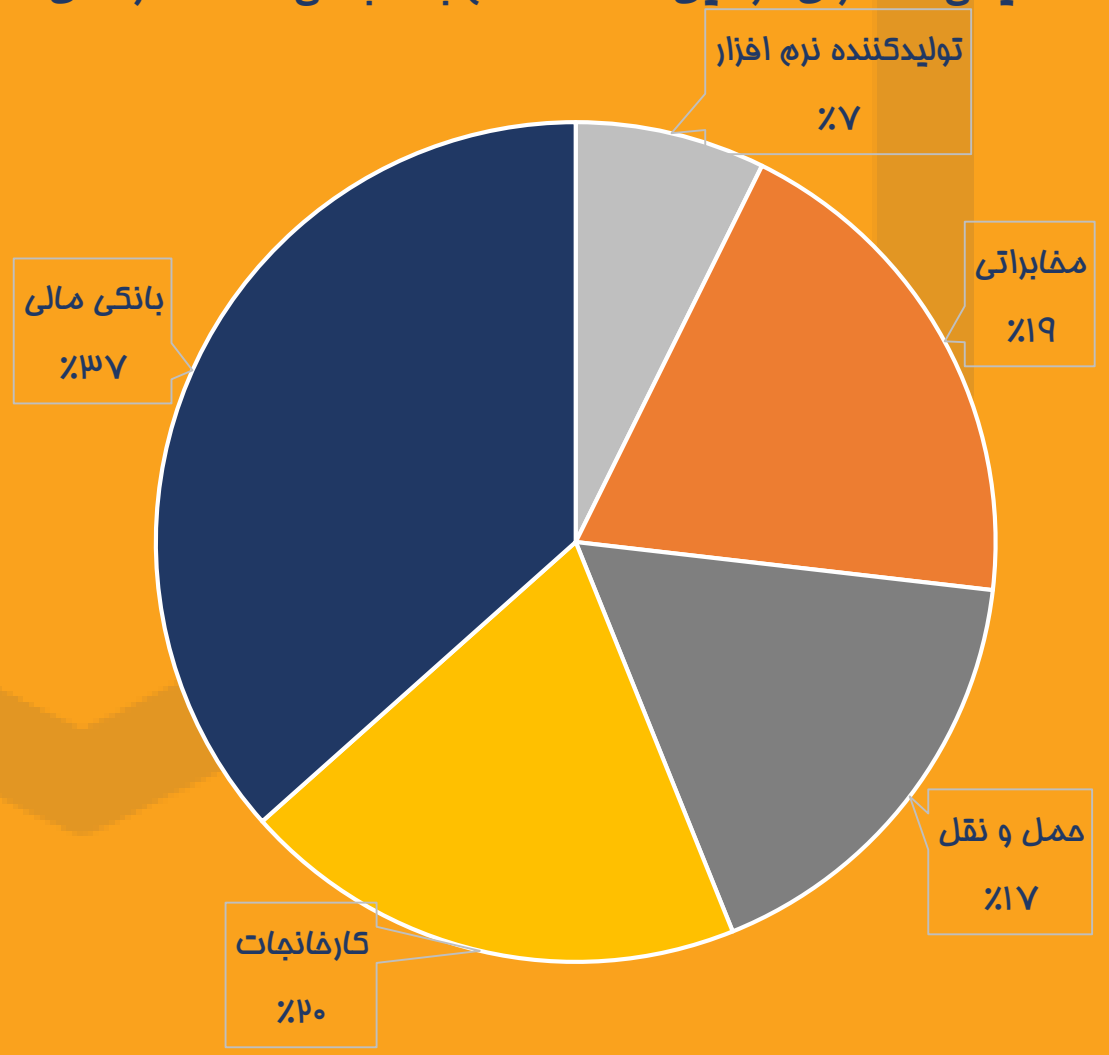
- HackerOne – www.hackerone.com
- Bugcrowd – www.bugcrowd.com
- Synack – www.synack.com/red-team
- Detectify – www.cs.detectify.com
- Cobalt – www.Cobalt.io
- Open Bug Bounty – www.openbugbounty.org
- Zerocopter – www.zerocopter.com
- YesWeHack – www.yeswehack.com
- HackenProof – www.hackernproof.com
- Vulnerability Lab – www.vulnerability-lan.com
- FireBounty – www.firebounty.com
- BugBounty.jp – www.bugbounty.jp
- AntiHack – www.antihack.me
- Intigriti – www.intigriti.com
- SafeHats – www.safehats.com
- RedStorm – www.redstorm.io
- Cyber Army ID – www.cyberarmy.id
- Yogosha – www.yogosha.com

متوسط عملکرد باگ بانتی در صنایع مختلف

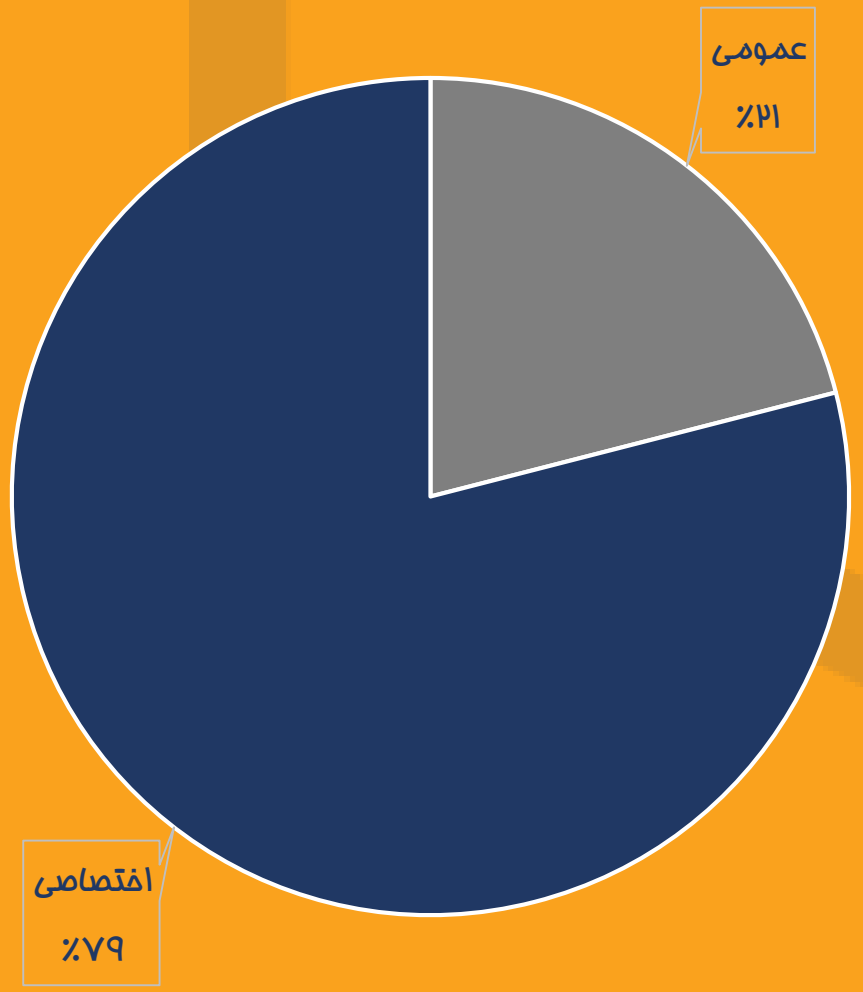


	زمان پرداخت بانتی	زمان ایمن سازی
آموزشی	2	62
هوا فضا	26	57
دولت	5	55
الکترونیک	17	25
سخت افزار	17	20
مخابرات	3	19
نرم افزار	6	17
خودرو	4	16
تجارت الکترونیک	3	13
سرگرمی	8	12
خدمات حرفه ای	2	12
بانکی	4	12
پزشکی	8	11
رمزارز	2	7
انرژی	1	2

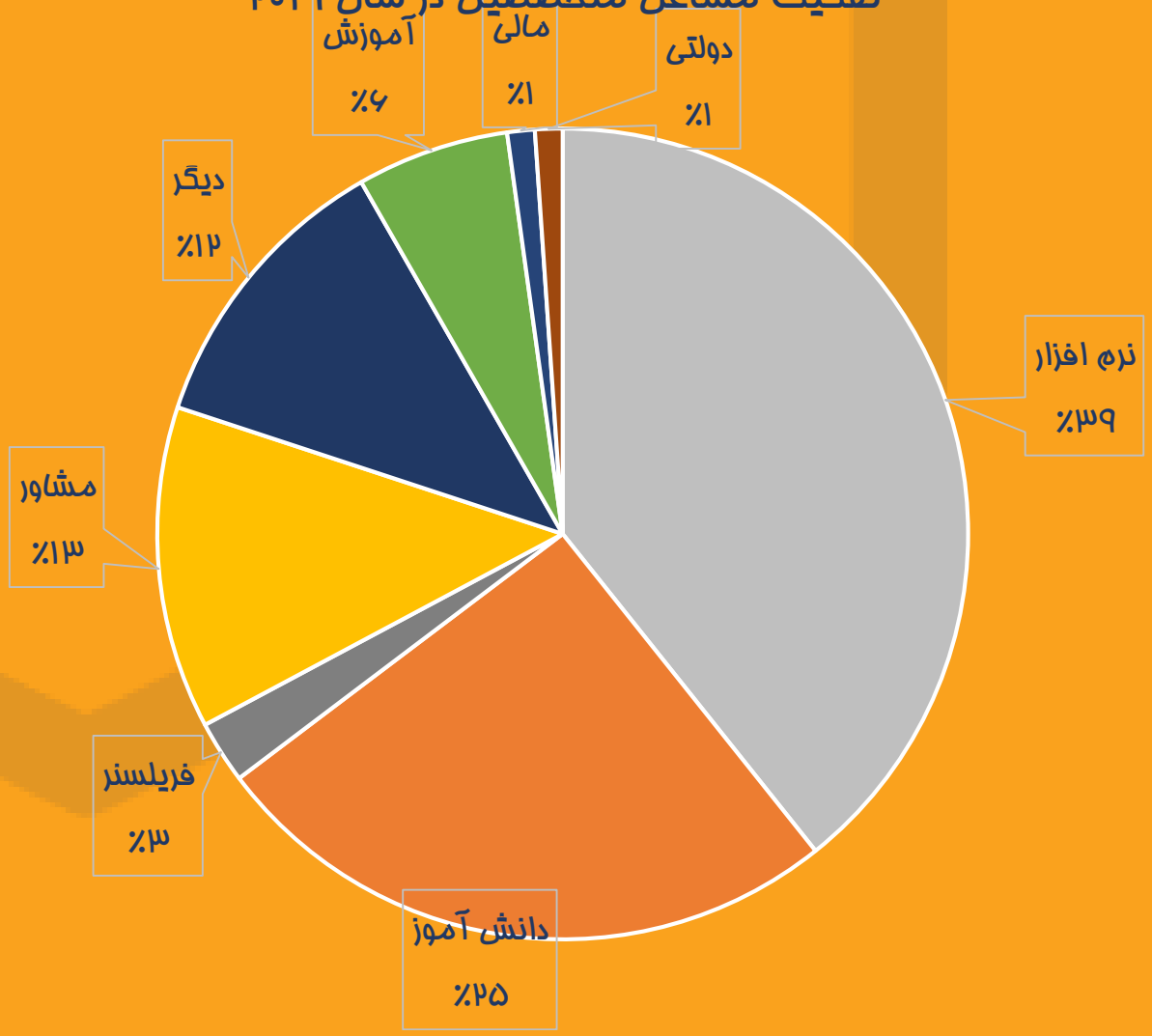
تفکیک صنایعی که دارای قوانین شفاف اعلام باگ بانتی هستند در سال ۲۰۱۹



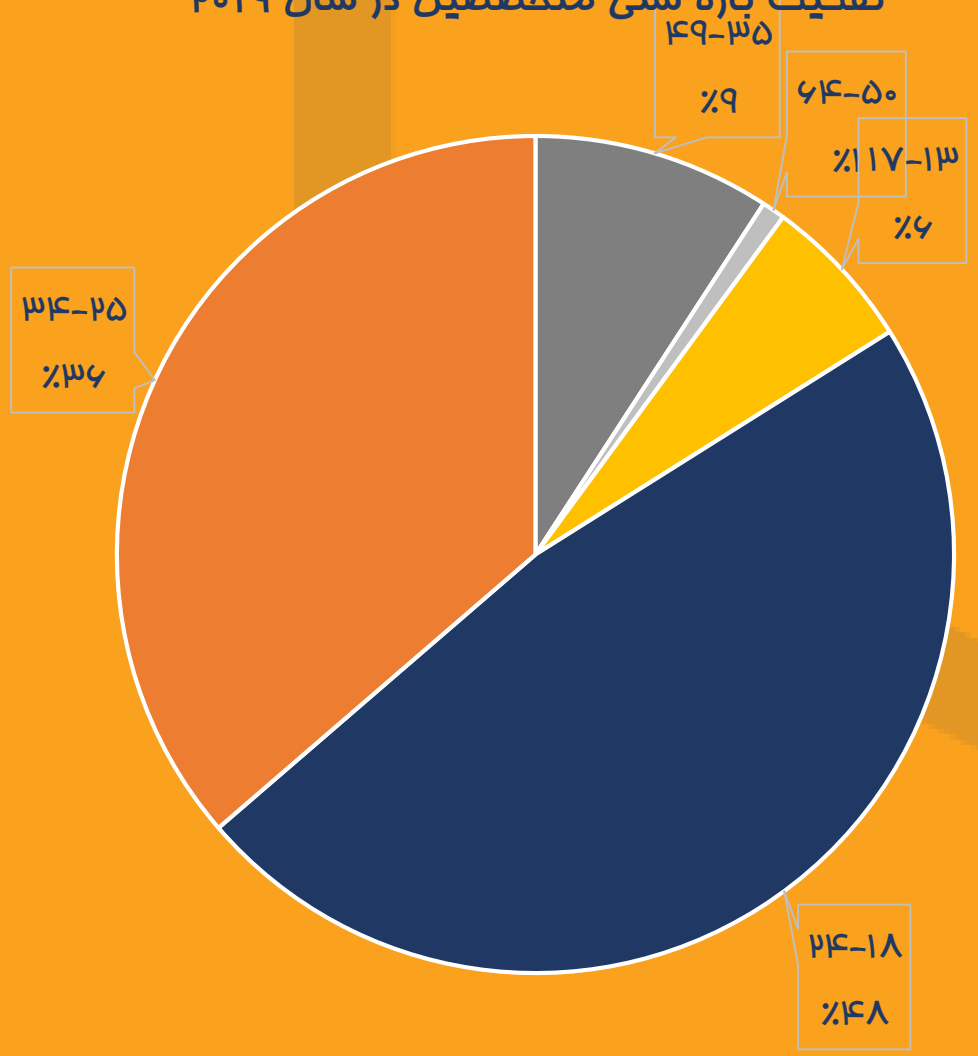
تفکیک نوع بانتی در سال ۲۰۱۹



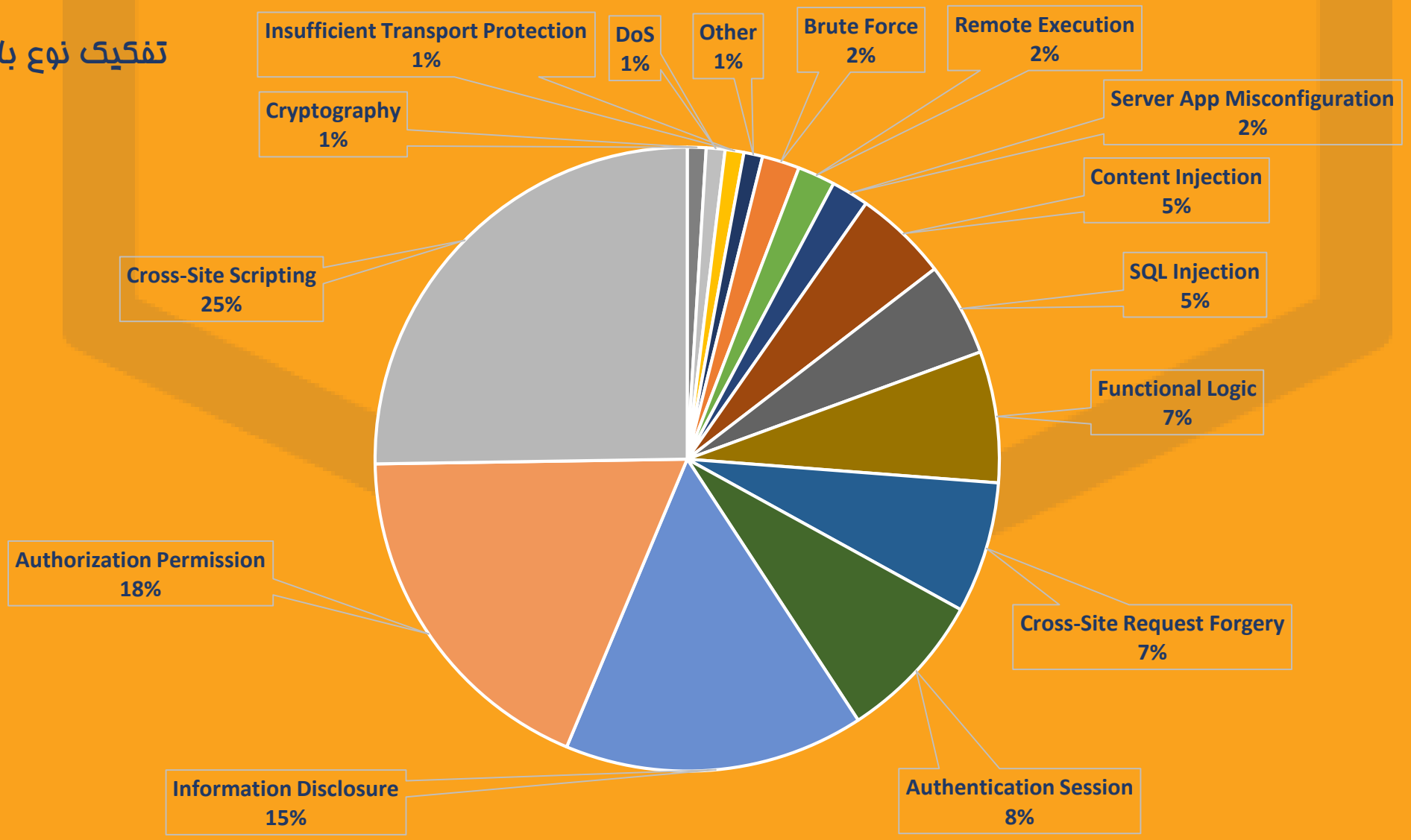
تفکیک مشاغل متخصصین در سال ۲۰۱۹



تفکیک بازه سنی متخصصین در سال ۲۰۱۹



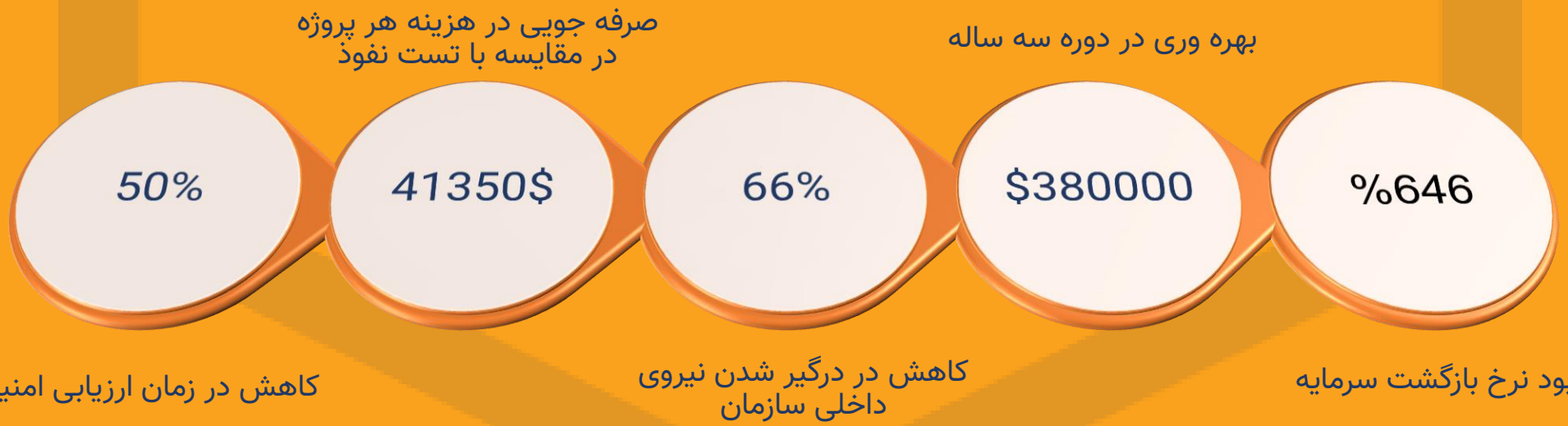
تفکیک نوع باگ در سال ۲۰۱۹



مزیت استفاده از باگ بانتی چیست؟

گزارشات و مستندات بین المللی در این باره چه می گویند؟

گزارش موسسه تحقیقات اقتصادی Forrester



این موسسه در آخرین مقالات خود در سال 2019 به بررسی نرخ بازگشت سرمایه برای سازمانهایی که از خدمات باگ بانتی استفاده نموده اند، پرداخته است.
بر اساس این گزارش، با استفاده از پلتفرم های باگ بانتی سازمان نیاز به جذب نیروی متخصص با نرخ دستمزد بالا بصورت تمام وقت را کاهش داده و از نتایج تست متخصصین بیشتر استفاده نموده است. همچنین دسترسی به گزارش فنی و شواهد باگ، زمان ایمن سازی را برای تیم توسعه کوتاه نموده است.
سازمان در هنگام شناسایی هر باگ دسترسی سریع به باگ خواهد داشت که بهینه سازی زمان ایمن سازی را در پی دارد.

مهمترین مشکلات فعلی سازمانها و دلیل استقبال از باگ بانتی

حداقل دستمزد کارشناس متخصص ارزیابی امنیتی بصورت متوسط 200 دلار در ساعت می باشد و معمولا امکان جذب و نگهداری این کارشناسان برای سازمانها وجود ندارد.
بیش از 84 درصد از سازمانها دارای فرآیندی یکپارچه برای تولید محصول ایمن نیستند.
وجود امور اداری و سازمانی مختلف برای کارشناسان داخلی سازمان، آنها را از اجرای ارزیابی امنیتی باز می دارد و از سوی دیگر اجازه تمرکز به توسعه توانمندیهای تخصصی و فنی را از آنها دلایل بوروکراسی های سازمانی می گیرد.

مهمترین دلایل کاهش بهره وری در پروژه های ارزیابی امنیت

- زمان ناکافی مورد نیاز برای اجرای ارزیابی امنیتی توسط متخصصین داخل سازمانی با توجه به حجم بالای توسعه ها و تغییرات در سامانه های سازمانی
- هزینه شناسایی، گردآوری، مدیریت، استخدام و نگهداری کارشناسان متخصص امنیتی
- به روز نبودن تیم داخلی نسبت به آخرین دانش و تهدیدات به دلیل بوروکراسی های سازمانی و نداشتن دیدگاه لزوم امنیت در مدیران سطح بالای سازمانی و پاسخگویی مدیر امنیت پس از وقوع رخدادهای امنیتی
- فرآیندهای پیچیده قراردادی، روالهای اداری بسیار برای اجرای پروژه های ارزیابی امنیتی

مزیت های ایجاد باگ بانتی برای سازمان

- متخصص امنیتی با ارایه باگ ها به سازمان کمک می نماید تا از وجود رخنه امنیتی با دسترسی سریع به باگ با هزینه مقرون به صرفه اطلاع یابد.
- سازمان دارای فرآیند مدیریت باگ می گردد و منابع آزاد شده از این بهره وری، برای ایمن سازی سریعتر محصولات اختصاص می یابد.
- سازمان به دلیل برون سپاری دریافت، تحلیل و تهیه راهکار گزارشات، زمان خود را بهینه می نماید و تبدیل به مخزنی از باگ های امنیتی نمی گردد و ریسک امنیتی سازمان کاهش می یابد.
- سازمان نیاز نیست در جستجوی افراد متخصص و متعهد و حرفه ای باشد و فرآیندهای پیچیده استخدامی و قراردادی را اجرا نماید و از همه مهتر نگهداری افراد متخصص از چالش ها و هزینه های سازمان کم می شود.
- سازمان زمان کمتری را برای جلسات تک به تک با هکرها خواهد گذاشت و بار زمانی پردازش گزارشات و حواشی مربوطه را به پلتفرم واسط برون سپاری می نماید که بهینه سازی زمان و بهره وری منابع برای سازمان را به دنبال دارد.
- سازمان می تواند بنابر اهمیت سامانه های خود از مزیت ارزیابی اجتماع متخصصین شناخته شده بصورت اختصاصی و VIP استفاده نماید تا درنتیجه چالش در معرض حملات بودن را کاهش دهد.

مزیت های ایجاد باگ بانتی برای سازمان

- باگ بانتی ها به دو صورت خصوصی و عمومی برگزار می شوند که سازمان به تناسب نیازمندیهای خود و سطح اهمیت تارگت ها می تواند انتخاب نماید.
- سازمان امکان مدیریت و انتخاب سطح گزارشات مورد نیاز خود را بنابر منابع و اولویت های کسب و کار خواهد داشت.
- تیم امنیت سازمان مملو از مستندات و گزارشات امنیتی نخواهد شد و تنها موارد با اهمیت برای کسب و کار در اولویت قرار می گیرند.
- تیم امنیت سازمان زمان خود را صرف مدیریت اجرای ارزیابی امنیتی نمی نماید و گزارشات موثق را دریافت می نماید.
- تیم توسعه و امنیت سازمان زمان خود را صرف ایمن سازی و توسعه محصول می نماید.
- سازمان دارای یک تیم مشاور و متخصص برای همکاری در تعیین تارگت ها، ارزشگذاری و ایمن سازی سامانه ها خواهد بود.
- مشاوران حقوقی پلتفرم باگ بانتی به سازمان کمک خواهند نمود تا قراردادها و مستندات مطابق با قوانین تایید شده توسعه یابد.

مزیت های ایجاد باگ بانتی برای متخصصین

- متخصصین امنیتی با استفاده از تخصص خود امکان افزایش درآمد خود را بصورت از راه دور خواهند داشت.
- ایجاد اجتماع متخصصین و تعامل با کمیته فنی محیطی حرفه ای و در احترام را ایجاد می نماید.
- متخصص امنیتی با ارایه گزارش باگ با پلتفرم باگ بانتی، درگیر چالش های قانونی با سازمان نخواهد شد.
- تیم حقوقی متخصص پلتفرم باگ بانتی زیرساخت سامانه و قراردادها را مورد بررسی و پایش قرار می دهند.
- متخصص امنیتی با ارایه گزارشات باگ حرفه ای و دارای ارزش، امکان عضویت در تیمهای اختصاصی پلتفرم را خواهد داشت.
- عضویت در تیمهای اختصاصی باگ بانتی منجربه افزایش درآمدزایی متخصص امنیتی با شیب بیشتر می گردد.
- متخصص امنیتی می تواند در صورت تمایل رزومه خود را برای جذب و استخدام در سازمانهای بزرگ استفاده نماید.
- متخصص امنیتی با فعالیت در پلتفرم باگ بانتی تبدیل به عضوی متخصص می گردد که درخواستهای بیشتر برای او در پی خواهد داشت.

ملاحظات قانونی و حقوقی باگ بانتی چیست؟

سازمانها و کسب و کارها در دیگر نقاط دنیا چه رویکردی برای حل این نگرانی داشته اند؟

ملاحظات و نگرانی های حقوقی سازمانها

- سازمانها نگرانی سواستفاده از اطلاعات باگ را دارا هستند، این چالش در خصوص تمام پروژه های امنیتی و گرفتن خدمات مطرح است.
- در دیگر نقاط دنیا به منظور بهره مندی از مزیت دسترسی سریع به مشکلات امنیتی، سازمانها آمادگی لازم برای ایمن سازی و وصله نمودن باگ های امنیتی را بصورت سریع مهیا می سازند.
- تنها شناسایی باگ و تبدیل شدن به مخزنی از آسیب پذیری ها، ریسک حقوقی سازمان را بالا میبرد.
- در صورتیکه سازمان قوانین و سیاست های خود را بصورت شفاف مشخص ننماید، قرارداد تست امنیتی می تواند برای سازمان و تیم تست ریسک حقوقی داشته باشد و هر دو دارای حواشی پیگیری های قضایی در قوانین مبهم و پیچیده خواهند شد که متاسفانه نتیجه این امر مبهم بوده و قابل پیش بینی نیست.
- توسعه قوانین بصورت کامل و جامع که از منظر حقوقی و فنی حامی سازمان و متخصص امنیتی باشد نیز از دیگر چالش های سازمانها می باشند.
- بسیاری از محققین و متخصصین در سراسر دنیا به دلیل ریسک هایی که به دلیل عدم شناخت و شفاف سازی سازمانها با باگ بانتی وجود دارد، آسیب پذیری های شناسایی شده را به سازمان اعلام نمی نمایند.
- مدیران سازمانها از سوی دیگر می دانند، آسیب پذیری های امنیتی غیرقابل اجتناب است و افشای اطلاعات سازمانها می تواند صدمات جبران ناپذیری را به کسب و کار وارد نماید و تنها با سرمایه گذاری بر روی فاز شناسایی می توانند امنیت را برای مشتریان خود ایجاد نمایند.

رویکرد کاهش ملاحظات حقوقی و قانونی

- برای اینکه سازمانها ریسک حقوقی خود را کاهش دهند، فرآیند پذیرش و ایمن سازی را شفاف و مشخص برای دریافت و پردازش باگ های امنیتی را تعریف می نمایند.
- در صورتیکه متخصص، مطابق با فرآیند شفاف پذیرش و ایمن سازی باگ که به او اعلام شده عمل ننمایند، سازمان می تواند مدعی حقوق قضایی خود باشد.
- این مساله در دیگر کشورها با توسعه برنامه اعلام آسیب پذیری یا VDP توسعه یافته است.
- سازمانهای بالغ و آگاه در زمینه امنیت سایبری در سراسر جهان دارای طرح VDP اختصاصی خود هستند تا بتوانند از مزیت های دسترسی سریع به اطلاعات باگ های امنیتی استفاده نمایند و از سوی دیگر سازمان و متخصصین امنیتی نیز در ریسک قرار نگیرند.
- طرح اعلام آسیب پذیری در واقع ایجاد انگیزه به اعلام مشکلاتی است که در سامانه های سازمان دیده می شود که شامل راهنما به متخصصین متعهد است که با پیروی از آن می توانند نسبت به اعلام باگ اقدام نمایند.
- هر طرح VDP قوانین و ملاحظات دقیق حقوقی و فنی را متناسب با شرایط سازمان نیازمند می باشد که در نتیجه متخصص و سازمان در محل امن قرار گیرند.
- طرح VDP می بایست با همکاری تیم حقوقی حرفه ای و تیم امنیتی متخصص تدوین و به روز شود در غیر اینصورت خود منشا ریسک امنیتی برای سازمان می گردد.

توسعه طرح اعلام آسیب پذیری یا VDP

- طرح VDP، نشان دهنده بلوغ امنیتی سازمان، نحوه تعامل با متخصص و پیروی از چارچوب های امنیتی است.
- این طرح نخستین بار توسط دپارتمان قضایی امریکا و اتحادیه اروپا انتشار و برای باگ بانتی الزامی شد.
- بر این اساس تمامی سازمانهایی که دارایی های اینترنتی دارند می بایست دارای طرح VDP باشند. در واقع به این معنا که اگر مشکلی را یافتید اعلام کنید. توسعه VDP نیازمند همکاری کارشناسان متخصص فنی و حقوقی است.
- موارد مهم در این طرح می بایست بصورت دقیق مشخص گردد مانند تعهد مدیران سازمان در قبال پیامد آسیب پذیری های امنیتی به مشتریان خود، دامنه مورد نظر سازمان برای اعلام باگ های امنیتی، چه فرآیندی برای اعلام باگ به سازمان باید طی شود، موارد استثنا و غیرقابل پذیرش و یا اولویت ها و نحوه ارزشگذاری آنها.
- در صورتیکه فرد شناسایی کننده و یا اعلام کننده باگ، مطابق با دستورالعمل شفاف سازمان عمل نماید، هیچ مشکل حقوقی برای فرد ایجاد نمی شود.
- پلتفرم های باگ بانتی در دنیا پیش از ارایه خدمات بانتی به سازمانها، خدمات توسعه VDP اختصاصی سازمان را در دستور کار قرار می دهند.

امنیت؛
به‌سبک باگدشت

BUGDASHT.ir
Bounty@BUGDASHT.ir
+98 21 42 71 92 90
in . , : BUGDASHT