بازبینی امنیتی و کشف آسیب پذیری

Security Audit and Vulnerability Scan

بازبینی امنیت سایبری

تیم ما یک روش چند لایه برای بررسی کد منبع در یک مکانیزم ماژولار برای اطمینان از پوشش کامل سطح برنامه و اصلاح کیفیت ارائه می دهد. بازبینی همواره برنامه های تولیدی میبایست از این استاندارد برای ایمن کردن برنامه خود استفاده کنند و یکبار توسط یک تیم امنیت سایبری بصورت کامل و جامع تمامی مکانیزم ها و سامانه های کدنویسی شده بررسی کامل و جامع شود چه بصورت دستی چه با عملیات های هوشمند.

بررسی امنیتی کد

روش نوآورانه ما برای سنجش کد منبع برای یک برنامه چارچوبی جامع را برای شناسایی نقص ها و مسائل امنیتی موجود در کد منبع در اختیار شما قرار می دهد. در روش بازبینی کد منبع، ما فقط به ابزارهای خودکار حسابرسی های کد منبع اعتماد نمی کنیم. ما از ترکیبی کامل از اتوماسیون و همچنین بررسی دستی کد منبع استفاده می کنیم تا تمام مناطق آسیب پذیر کد منبع را پوشش دهیم .این بررسی به دقت و با حضور ذهن کامل در کارشناسان ما طبق چک لیستی کامل صورت خواهد گرفت.

بازبینی امنیتی

در خدمات بازبینی امنیتی و کشف آسیب پذیری خدماتی که ارائه می شود در راستای امن سازی داخلی نرم افزارها، پیکربندی های نادرست، مراودات درون شبکه ای و بررسی کد منع نرم افزار، که تمامی اینها طبق روش های نوین روز دنیا و تکنیک های استاندارد پیاده سازی خواهد شد، برای مثال بهره گیری از جستجوگر های موفق در دنیا مانند AFL و ASAN که در کشف آسیب پذیری های سطح باینری از کار آمدی خوبی برخودار هستند، همچنین در ابعاد برنامه های تحت وب از جستجوگرهای بومی خود برای کشف آسیب پذیری جعبه سیاه و جعبه سفید استفاده نموده و ارزیابی های انسانی را در نهایت بدست کارشناسان خبره خود انجام خواهد داد.

راه ارتباطی

تلفن:
026 368 06249

وبسایت:
unk9vvn.com

ایمیل:
info@unk9vvn.com

بررسی امنیتی تنظیمات

بررسی پیکربندی و بررسی ساخت در فضاهای نرم افزاری مانند سیستم عامل ها، سرویس ها) به عنوان مثال (HTTP انجام می شود. ما پیکربندی مربوط به امنیت را براساس معیارهایی مانند NIST ، CISو توصیه های مشتری تأیید می کنیم.همچنین نرم افزار مربوطه را در فضاهای مختلف در آزمایشگاه خودمان راه اندازی کرده و در شرایط های مختلف بررسی صفر تا صدی را انجام میدهیم.

بازبینی امنیتی IT

بازبینی امنیتی IT به معنیه بررسی ارتباطات و پروتکل های مورد استفاده که در جریان ایجاد یک شبکه استفاده می شود. همچنین سرویس هایی که بر بستر شبکه فعالیت میکنند مانند Active Directory و SMB Serverکه در صورت اشتباه در پیکربندی آنها میتواند خسارت های جبران نا پذیری را برای قربانی به همراه داشته باشد. از دیگر مواد مورد بررسی میتوان به پیکربندی و طراحی قوانین برای روترها و سوئچ های درون شبکه ای اشاره کردن که تمامی آنها میبایست بررسی های امنیتی را انجام دهند.

جستجوی آسیب پذیری

ما فرآیند رویکرد جعبه سفید را برای انجام بررسی امنیتی کد منبع دنبال می کنیم که با درک که از چگونگی ساخت برنامه ها پیدا می شود و اطمینان از پیروی از شیوه های کدنویسی ایمن در طول چرخه عمر توسعه نرم افزار تمرکز می کنیم .چنین رویکرد ارزیابی زمینه ای متفاوت است که بصورت تجزیه و تحلیل ایستا خواهد بود و به دنبال الگوهای آسیب پذیری عمومی هستنم .علاوه بر این، ما چنین بررسی هایی را با راهنمایی های عملی در راستای امن سازی است و مخصوص طراحی، پلتفرمها و تکنولوژی های اجرایی متفاوت هر برنامه به صورت موردی خواهیم داد .

بررسی امنیت کار از راه دور

ما ارزیابی های امنیتی کار را از تنظیمات خانه (WfH) انجام می دهیم. در سمت کاربر / کارمند بررسی زیرساخت سیستم و بررسی پیکربندی را می توان انجام داد. علاوه بر این، برنامه های مورد استفاده برای تماس های کنفرانسی، پیام رسانی، سرویس گیرندگان VPNو سایر برنامه های معمولی مورد استفاده در سناریوی کار از راه دور قابل ارزیابی هستند.

در سمت کارفرما می توانیم وضعیت امنیتی زیرساخت های خارجی را که مسئول دسترسی از راه دور هستند، آزمایش کنیم مانند سرورهای VPN.

آنالیز امن سازی کد

یکی از موارد استاندارد در تولید یک محصول نرم افزاری فرایند امن سازی و بازرسی کدهای توسعه توسط برنامه نویسان خواهد بود، که خود این امر میبایست توسط تیم های حرفه ای مورد بازبینی کامل تر و دقیق تری قرار گیرد تا خطر آسیب پذیری های پیشرفته و جدید را به حداقل برساند.

این بررسی در راستای عملکرد صحیح استانداردسازی کد بوده و تلاش دارد تا اگر ضعف هایی در روند امن سازی مشاهده شد رفع و حل نماید، کیفیت الگوریتم ها بروز بودن آنها و منطق طراحی همواره از شاخصه های اصلی این ارزیابی بوده اند.

قوانین پیکربندی های امنیتی

در بازبینی امنیتی بعد از گذراندن موارد ذکر شده در امر ایمن سازی برنامه و سامانه مربوطه میبایست دستورالعمل هایی مبنی بر تعیین سیاست ها و چهارچوب های مورد تایید از لحاظ امنیتی بر اساس سرویس دهی مشتری تدوین و مستند سازی شود.

این امر میتواند تیم پشتیبانی را در توسعه همواره از انجام خطاهای سطح خطرناک ایمن باقی نگاه داشته و نکات مهم را در توسعه پلتفرم های خود بخوبی رعایت بفرمایند. همچنین از بکار بردن توابع خطرناک در موقعیت های اشتباه استفاده نکرده و ریسک خطر را به پایین ترین سطح برساند.