بازبینی امنیتی و کشف آسیب پذیری

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. برنامه های تولیدی میبایست از این استاندارد برای ایمن کردن برنامه خود استفاده کنند و یکبار یک تیم امنیت سایبری بصورت دستی یا با عملیات های هوشمند تمامی مکانیزم ها و سامانه های کدنویسی شده آن را به صورت کامل بررسی نماید.

بررسی امنیتی کد

روش نوآورانه ما برای سنجش کد منبع یک برنامه، چارچوبی جامع برای شناسایی نقص ها و مسائل امنیتی 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 ترکیب کامل 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 و طبق چک لیستی صورت خواهد گرفت.

بازبینی امنیتی

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

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 آن را در شرایط مختلف بصورت صفر تا صد بررسی میکنیم.

بازبینی امنیتی IT

بازبینی امنیتی IT به معنی بررسی ارتباطات و پروتکل های مورد استفاده است که در جریان ایجاد یک شبکه استفاده می شوند. همچنین سرویس هایی که بر بستر شبکه فعالیت میکنند مانند Active Directory و SMB Server، در صورت اشتباه در پیکربندی آنها خسارت های جبران ناپذیری را میتواند برای قربانی به همراه داشته باشد. از دیگر مواد مورد بررسی پیکربندی و طراحی قوانین برای روترها و سوئیچ های درون شبکه ای است 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 و با درکی که از چگونگی ساخت برنامه ها پیدا می شود و اطمینان از پیروی از شیوه های کدنویسی ایمن در طول چرخه عمر، برروی 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 میباشد. علاوه بر این، ما چنین بررسی هایی را با راهنمایی های عملی در راستای امن سازی قرار میدهیم و پلتفرم ها و تکنولوژی های اجرایی را بصورت متفاوت در هر برنامه خواهیم داشت.

بررسی امنیت کار از راه دور

ما ارزیابی های امنیتی کار را از تنظیمات خانه (WfH) انجام می دهیم. بررسی زیرساخت سیستم و بررسی پیکربندی را می توان در سمت کاربر / کارمند 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 توان وضعیت امنیتی زیرساخت های خارجی که مسئول دسترسی از راه دور هستند، مانند سرورهای VPN را آزمایش کنیم.

آنالیز امن سازی کد

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

این بررسی در راستای عملکرد صحیح استاندارد سازی 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 هستند.

قوانین پیکربندی های امنیتی

بعد از گذراندن موارد ذکر شده در امر ایمن سازی برنامه و سامانه مربوطه میبایست دستورالعمل هایی مبنی بر تایین 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 از انجام خطاهای سطح خطرناک ایمن نگه داشته و نکات مهم را در توسعه پلتفرم های خود بخوبی رعایت کند. همچنین از بکار بردن توابع خطرناک در موقعیت های اشتباه استفاده نکرده و ریسک خطر را به حداقل میرساند.