Cyber Resilience پاسخ‌گویی سیستماتیک به حملات هکری

انعطاف‌پذیری سایبری چیست و کاربرد آن در دنیای امنیت چگونه است؟

پیشگیری از وقوع حملات سایبری به معنای کم کردن احتمال نفوذ به زیرساخت‌های ارتباطی است. متخصصان امنیتی می‌دانند که هیچ سامانه‌ای در برابر تهدیدات امنیتی ایمن نیست و هر لحظه ممکن است سامانه‌های امنیتی یک حمله هکری را شناسایی کنند. سازمان‌ها برای کم کردن آثار مخرب یک حمله سایبری به سراغ الگوی انعطاف‌پذیری سایبری (Cyber Resilience) رفته‌اند. انعطاف‌پذیری سایبری سعی می‌کند با ارائه یک مکانیزم مدیریت مخاطرات (Risks) سایبری، شدت آسیب‌های وارد شده به یک سامانه را به حداقل برساند. انعطاف‌پذیری سایبری از تکنیک‌های رایج برای شناسایی و پیشگیری از بروز حملات استفاده می‌کند، اما احتمال نفوذ را منتفی نمی‌داند، به همین دلیل سعی می‌کند با پیش‌بینی، واکنش سریع و تطبیق‌پذیری با شرایط پس از حمله میزان تخریب را به حداقل برساند.

آزمایشگاه NSS پژوهشی انجام داده که نشان می‌دهد بیشتر محصولات امنیتی پیشرو در صنعت سایبری اگر به درستی استفاده شوند مفید هستند. در این پژوهش 10 سامانه پیشگیری از نفوذ آزمایش شدند تا عملکرد آن‌ها در مواجه با نفوذ به شبکه بررسی شود. این آزمایش نشان داد که سامانه‌های پیشگیری از نفوذ در ارتباط با شناسایی اکسپلویت‌ها، مقابله با نفوذ بدافزارها به درون سامانه‌ها (گریز از مکانیزم‌های امنیتی) و قابلیت اطمینان در 94 درصد موارد موفق ظاهر می‌شوند. در این پژوهش 9 عدد از محبوب‌ترین دیوارهای آتش نسل بعد (NGFW) که قادر به شناسایی ترافیک‌های مشکوک بودند بررسی شدند که 8 مورد از آن‌ها در رابطه با میزان اثربخشی امنیتی امتیاز بالاتر از 90% را کسب کردند. بالاترین امتیاز کسب شده در ارتباط با میزان اثربخشی برابر با 98.5% درصد بود. NSS می‌گوید: «اثربخشی امنیتی به میزان 98.5 درصد را نباید یک امتیاز خوب در نظر گرفت، زیرا بیشتر حملات موفقیت‌آمیز بر مبنای 1.5 درصد حملات کشف نشده پیاده‌سازی می‌شوند. اگر تنها کسری از 1.5 درصد تهدیدات توسط دیوارهای آتش نسل بعد، سامانه‌های پیشگیری از نفوذ یا سامانه‌های محافظت از نقاط پایانی شناسایی نشوند، سرآغازی بر یک نفوذ است.» فعالیت‌های مخرب سایبری امروزی حول محور ساخت درب‌های پشتی قرار دارند تا هکرها بتوانند به منابع یک سازمان دسترسی پیدا کرده، سطح دسترسی‌های خود را افزایش داده و اطلاعات حساس را استخراج کرده یا اختلالی در فعالیت‌های سازمان به وجود آورند. به همین دلیل مهم است که مهندسی سامانه‌ها و معماری سازمانی مبتنی بر مدیریت مخاطرات امنیتی باشد تا کارشناسان امنیتی بتوانند از عملکرد صحیح زیرساخت‌های ارتباطی اطمینان حاصل کنند.»

مشاهدات آزمایشگاه NSS

سازمان‌های کوچک و بزرگ مجهز به سامانه‌های امنیتی در برابر 98.5 درصد از تهدیدات ایمن هستند، تنها 1.5 درصدی که توسط ابزارهای امنیتی شناسایی نمی‌شوند به زیرساخت‌ها خسارت‌های سنگین وارد می‌کنند.
انعطاف‌پذیری امنیت سایبری سامانه‌ها و شبکه‌ها با هدف حصول اطمینان از کارکرد درست سامانه‌ها در یک محیط متاثر از نفوذ تدوین می‌شود.

کارشناسان امنیتی نباید به کنترل‌ها و سنجه‌های امنیتی به عنوان یک راهکار کاملا ایمن در برابر تهدیدات نگاه کنند، زیرا کنترل‌های امنیتی با هدف کاستن از صدمات امنیت سایبری استفاده می‌شوند. پویش آسیب‌پذیری‌ها برای شناسایی مخاطرات احتمالی به تنهایی کافی نیست و باید اقدامات مکمل دیگری همچون آزمون‌های نفوذپذیری روی تجهیزات هوشمندی که قرار است به شبکه اضافه شوند انجام شود. سازمان‌ها باید روی زمان شناسایی و پاسخ‌گویی به حملات متمرکز شوند تا سامانه‌ها بتوانند پس از شناسایی حمله به زیرساخت‌های ارتباطی با 60 درصد ظرفیت موجود باز هم کار کنند، حتا اگر دسترسی به برخی از سرویس‌های کلیدی امکان‌پذیر نباشد. سازمان‌ها برای کاهش نفوذ به زیرساخت‌های ارتباطی باید برای پرسش‌های زیر پاسخ مناسبی داشته باشند.

- هکرهای امروزی از چه بردارهای حمله برای نفوذ استفاده می‌کنند؟
- کدامیک از بردهای حمله می‌توانند استراتژی‌های مهم کسب‌وکار را با مشکل روبرو کنند؟
- چه بردارهای حمله‌ای می‌توانند از سامانه‌های دفاعی پیاده‌سازی شده عبور کنند؟

استراتژی انعطاف‌پذیری سایبری به این اصل مهم اشاره دارد که پس از شناسایی یک حمله لازم است بخش‌های آلوده شبکه ایزوله شوند تا منابع کلیدی و سالم بتوانند به کار خود ادامه دهند. برای نیل به این هدف باید شبکه یا شبکه‌ها به بخش‌های مختلفی تقسیم شوند تا یک میزبان آلوده با اولویت پایین نتواند تمامی شبکه یک سازمان را آلوده کرده و باعث از دست رفتن کل سیستم شود. زمانی که شبکه‌ای تحت تاثیر یک نفوذ سایبری قرار می‌گیرد، امکان بازگرداندن شبکه به حالت اولیه در کوتاه‌مدت فراهم نیست. استراتژی ایزوله‌سازی بخش آلوده شبکه اجازه می‌دهد، زمانی که حمله همچنان در حال اجرا است به واکاوی این موضوع بپردازید که چرا حمله موفقیت‌آمیز بوده و در ادامه معماری شبکه را به گونه‌ای باز طراحی کنید که در مقابل حملات مشابه ایمن باشد. دقت کنید در زمان پیاده‌سازی حمله به یک شبکه ایزوله شده به سرعت دسترسی هکر به شبکه را قطع نکنید و اجازه دهید هکر کار خود را ادامه دهد تا اطلاعات بیشتری به دست آورید. این اطلاعات در زمان ارائه به مجامع قضایی کمک فراوانی می‌کند.

مطلب پیشنهادی

مقابله با تهدیدات مهندسی اجتماعی
13 نمونه واقعی از حملات فیشینگ و راهکار مقابله با آن‌ها

تجزیه و تحلیل داده‌ها

یکی از موثرترین روش‌های محافظت از سامانه‌ها در برابر تهدیدات سایبری به‌کارگیری محصولات امنیتی در سطح شبکه و نقاط پایانی بر مبنای استراتژی دفاع در عمق است. استراتژی فوق بر مبنای این فرضیه آماده می‌شود که تفاوت مشخصی میان شبکه داخلی و خارجی وجود دارد. کارشناسان امنیتی در این زمینه نقل قول معروفی دارند که اعلام می‌دارند: «ساخت دیوارهای بلند و حفر خندق در پشت دیوار زمانی منطقی است که ارزشمندترین دارایی‌های سازمان در اعماق قلعه نگه‌داری شود.» لازم است مکانیزم‌های امنیتی به شکل لایه‌بندی پیاده‌سازی شوند تا ساختار دفاعی شبکه مستحکم‌تر شوند. یک استراتژی امنیتی خوب بر مبنای محاسبات ریاضی پیاده‌سازی می‌شود. در روش فوق نرخ شکست ترکیبی محصولات مختلف از طریق ضرب میزان شکست همه محصولات به دست می‌آید. به‌طور مثال، اگر IPS یک سازمان اجازه 1 حمله از میان 100 حمله و دیوارآتش نسل بعد اجازه 1 حمله از میان 100 حمله را می‌دهد، در مجموع محصولات فوق باید تنها اجازه پیاده‌سازی موفقیت‌آمیز یک حمله در 10 هزار حمله را بدهند (0.01 x 0.01). آزمایشگاه NSS می‌گوید: «محاسبه فوق سطح امنیتی استراتژی دفاع در عمق را خوش‌بینانه نشان می‌دهد، اما واقعیت چیز دیگری است، زیرا بدافزارهای نسل جدید و پیشرفته می‌توانند با استفاده از ترفندهای خاصی از سد محصولات امنیتی عبور کنند. ورود خدمات ابری و استفاده فراگیر دستگاه‌های همراه باعث شده استراتژی‌های سنتی دفاع در عمق کارایی کمی داشته باشند، زیرا دستگاه‌های ارتباطی مختلف به کارمندان یک سازمان اجازه می‌دهند به‌طور مداوم اطلاعات را به خارج از شبکه سازمانی ارسال کنند.»

مطلب پیشنهادی

وقتی یک تحلیلگر امنیتی برای آزمایش سطح دفاعی یک مرکز بازپروری نزدیک‌ترین فرد به خود را انتخاب می‌کند.
چگونه مادر یک هکر مخفیانه به یک زندان و کامپیوتر سرپرست آن نفوذ کرد

ناکارآمدی برخی از مکانیزم‌های امنیتی

کارشناسان امنیتی گاهی اوقات خط‌مشی‌های امنیتی که شامل اقدامات مناسب در قبل و بعد از یک نفوذ است را بازبینی می‌کنند. رویکرد فوق شامل طراحی، نظارت و مدیریت کنترل‌های امنیتی مناسب است که ترافیک شبکه داخلی را زیر نظر می‌گیرند تا در کوتاه‌ترین زمان نفوذ به شبکه شناسایی شود و اگر ساختارهای امنیتی نیازمند بازنگری هستند بر مبنای اطلاعات جدید تغییرات به سرعت اجرایی شوند تا آسیب‌های کمتری به زیرساخت‌ها وارد شود. آزمایشگاه NSS می‌گوید: « دنیای امنیت اطلاعات شاهد شکل‌گیری رویکرد نوینی است، مبنی بر این‌که کارشناسان امنیتی نباید روی 98.5 درصد حملاتی که ابزارهای امنیتی قادر به شناسایی آن‌ها هستند تمرکز کنند، بلکه باید روی 1.5 درصد حملاتی که مستتر هستند و سامانه‌های دفاعی اجازه ورود آن‌ها به شبکه را می‌دهند متمرکز شوند. دقت کنید، تمامی راهکارهای امنیتی، حتا فناوری‌های شناسایی نفوذ، در شناسایی برخی از حملات با شکست روبرو می‌شوند. سازمان‌ها نباید اکوسیستم امنیت امروزی را به عنوان یک مکانیزم دفاعی کاملا مستحکم در برابر حملات تصور کنند، بلکه باید به عنوان یک لایه امنیتی به آن‌ها نگاه کنند و پس از استقرار مکانیزم امنیتی در قالب دکترین دفاعی آسیب ناشی از حمله را مدیریت و سعی کنند نفوذ واقعی به یک شبکه را به حداقل برسانند تا تیم‌های واکنش سریع بتوانند با تهدیدات مقابله کرده و آسیب وارد شده به خدمات و تجهیزات را برطرف کنند. سازمان‌ها برای دفاع در برابر تهدیدات نوین باید به‌طور مستمر راهکارهای فعلی را آزمایش کنند تا مکانیزم‌هایی که بهره‌وری را افزایش داده و هزینه‌ها را کاهش می‌دهد برای دفاع از زیرساخت‌های شبکه استفاده شود. برای ایمن‌سازی زیرساخت‌های یک سازمان بزرگ همچون یک ارائه‌دهنده خدمات اینترنت می‌توان از Air-Gap یا ترکیبی از گیت‌وی‌های امنیتی یک طرفه در تعامل با تجهیزات ایمن‌سازی ByPass میان زیرساخت‌های حساس و شبکه‌های ارتباطی استفاده کرد تا خطرات ناشی از حملات هکری به حداقل برسد. سازمان‌ها باید فناوری‌هایی همچون ظرف عسل را بازنگری کنند تا هزینه حمله به زیرساخت‌ها برای هکرها افزایش یابد. راهکار فوق نمی‌تواند به‌طور قاطع مانع هکرها شود یا حمله‌ای را خنثا کند، اما به بهبود ساختار شبکه کمک فراوانی می‌کند.»

مطلب پیشنهادی

پخش زنده و آنلاین دربی استقلال و پرسپولیس

پویش آسیب‌پذیری‌ها با کمک Threat Intelligence

تیم‌های امنیتی به ابزارها و راهکارهای جالبی همچون اسکنرهای نقاط آسیب‌پذیر، فیدهای اعلام کننده تهدیدات و زیرساخت‌های هوشمند امنیتی برای مقابله با تهدیدات دسترسی دارند که عملکرد نسبتا خوبی دارند، اما نباید از این نکته غافل شد که مشکلات متعدد هر یک از ابزارهای یاد شده مانع از آن می‌شود تا تیم‌های امنیتی بتوانند به شکل مناسبی از آن‌ها استفاده کنند. به‌طور مثال Thread Feedها زمانی که یک آسیب‌پذیری شناسایی شده یا اطلاع‌رسانی درباره یک اکسپلویت به شکل عمومی انجام شده گزارش مربوطه را برای تیم‌های امنیتی اعلام می‌کنند. به عبارت دیگر، ابزارها می‌توانند درباره یک تهدید اطلاع‌رسانی کنند تا سازمان‌ها بتوانند وصله‌های مربوطه را نصب کنند، اما توانایی مشخص کردن هدف را ندارند. آزمایش انجام شده توسط آزمایشگاه NSS نشان داد مکانیزم‌های هشداردهنده در ارتباط با به‌روزرسانی Java 6 Update 23 عملکرد صددرصدی دارند، اما در ارتباط با به‌روزرسانی Java 7 Update 2
این میزان به کمتر از 5 درصد رسید. تمرکز بیش از اندازه روی گزارش‌های ورودی و اطلاعات دریافتی از سامانه Security Information And Event Management (SIEM) سرنام باعث شکل‌گیری یک نگرش اشتباه شده و کمک چندانی به بهبود مکانیزم‌های دفاعی نمی‌کند. سوال مهم این روزهای امنیت این نیست که چه تهدیدی توسط

سیستم دفاعی شناسایی شده، بلکه سوال این است که چه تهدیدی توانسته از سامانه دفاعی عبور کند. مشکل اصلی این است که ابزارهای امنیتی در ارتباط با فعالیت‌های مشکوکی که قادر به شناسایی آن‌ها نیستند هیچ گزارش یا هشداری ارائه نمی‌کنند. به همین دلیل تلاش برای پیدا کردن مکانی که نقطه شروع نفوذ بوده و آسیبی که به سامانه‌ها وارد شده کار سختی است. هکرها زمانی که متوجه شوند چه ابزارهای امنیتی در شبکه یک سازمان نصب شده، به سراغ پیدا کردن آسیب‌پذیری‌های مستتر در محصولات امنیتی می‌روند، به همین دلیل محصولات امنیتی به جای آن‌که به مقابله با هکرها بپردازند، آن‌ها را به سمت اهدافی که امنیت پایین‌تری دارند هدایت می‌کنند! در بیشتر موارد نفوذ زمانی انجام می‌شود که هکر هر روی یک برنامه کاربردی که سازمان از آن استفاده می‌کند و کنترل‌های امنیتی قادر به متوقف کردن حمله نیستند، متمرکز می‌شود.

مطلب پیشنهادی

علاج بعد از وقوع حادثه
چه باید کرد اگر اطلاعات محرمانه ما افشا شود

کشف اکسپلویت‌های احتمالی

کارشناسان امنیتی برای تشخیص این‌که هکرها قبل از نفوذ به یک سازمان ممکن است تمرکز خود را روی کدامیک از بردارهای حمله قرار دهند باید به این اصل مهم دقت کنند که باید اطلاعات کاملی در ارتباط با روش‌ها و بردارهای حمله جمع‌آوری کرد. این اطلاعات می‌توانند در ارتباط با تجهیزات زیرساختی شبکه همچون سرورها، نقاط پایانی، برنامه‌های کاربردی و سایر دارایی‌های سازمان باشد. اطلاعات یاد شده کمک می‌کنند تا بتوان لایه‌های آسیب‌پذیر را شناسایی کرد. اگر سازمانی به دلیل یک اکسپلویت جاوا در معرض تهدید باشد، اما سامانه تشخیص نفوذ قادر به شناسایی و متوقف کردن اکسپلویت باشد، در این حالت سازمان در معرض مخاطرات پیرامون اکسپلویت قرار نگرفته و نشان می‌دهد اثربخشی کنترل‌های امنیتی در حد مطلوبی قرار دارند. زمانی‌که سامانه یا زیرساختی تحت تاثیر یک نفوذ قرار گرفت، اولین موضوعی که باید بررسی شود، مدت زمانی است که سامانه یا زیرساخت تحت تاثیر حمله قرار داشته و سازمان متوجه این مسئله نشده است. تشخیص این مسئله که یک سرور تحت تاثیر یک حمله بدافزاری قرار گرفته کافی نیست، زیرا برطرف کردن مشکل در بیشتر موارد کار ساده‌ای است، نکته مهم شناسایی ابعاد حمله و مدت زمانی است که زیرساخت‌ها تحت تاثیر حمله قرار داشته‌اند. هر چه زمان بیشتر باشد، اطلاعات مهمی به بیرون نشت پیدا کرده است. تیم‌های امنیتی که تنها هدف آن‌ها متوقف کردن ترافیک مخرب یا دفع حمله است، در بیشتر موارد به درستی متوجه نمی‌شوند سرویس‌ها چه مدت زمانی تحت تاثیر حمله بوده‌اند. شناسایی حملات اولیه یا تشخیص آلودگی ساختار شبکه مهم نیست، زیرا مشکل اصلی بروز اختلال در سرویس‌ها یا از دست رفتن داده‌های مهم است. مهم‌ترین اصل پیرامون انعطاف‌پذیری سایبری درک این مسئله است که نفوذ به هر شبکه‌ای اجتناب‌ناپذیر است و سازمان‌ها باید به دنبال کاهش نفوذ باشند. انعطاف‌پذیری سایبری به سازمان‌ها اجازه می‌دهد حتا در زمان بروز حملات مستمر و مداوم بازهم به ارائه سرویس‌ها و خدمات کاربری بپردازند. به همین دلیل به جای آن‌که هزینه بی‌موردی صرف متوقف‌سازی حملات برون و درون سازمانی شود، باید تهمیدات دفاعی در نظر گرفته شود تا حتا در زمان بروز حمله اختلالی در کارکرد خدمات به وجود نیاید.

مطلب پیشنهادی

راهنمای جامع استقرار و کار با Honeypot
با یک ظرف عسل امنیت شبکه خود را افزایش دهید

خط‌مشی پیشگیرانه به جای پاسخ‌های واکنش‌گرا

در حالت ایده‌آل، بررسی دقیق آسیب‌پذیری‌های مستتر در کنترل‌های امنیتی باید از رویکرد ارزیابی لحظه‌ای به ارزیابی مستمر تغییر پیدا کند تا یک الگوی بلادرنگ (Real-time) به دست آید. امروزه بیشتر استراتژی‌های امنیتی که

پیاده‌سازی می‌شوند دارای نقایصی هستند که نادیده گرفتن احتمال نفوذ در هر زمان یکی از این موارد است. آیا اکسپلیوت‌هایی که برای حمله به لایه‌های دفاعی از آن‌ها استفاده می‌شود تنها در سرویس‌های کاربردی سازمان قرار دارند یا درون محصولات امنیتی نیز قرار دارند؟ تنها با شناسایی دقیق اکسپلویت‌های ارسال‌کننده بدافزار به یک نقطه پایانی می‌توان میزان پایداری یک مدل خاص را ارزیابی کرد. جمع‌آوری اطلاعاتی در این سطح اجازه می‌دهد اثربخشی ابزارهای حفاظتی همچون IPSها، EEPها و میزان خطرپذیری نقاط پایانی را ارزیابی کرد. سازمان‌ها می‌توانند از اطلاعات فوق برای محاسبه سطح ریسک بر مبنای مشخصات سازمان که شامل ریسک نفوذ، خدمات، وابستگی‌ها، نیازهای عملیاتی و دارایی‌های مهم می‌شوند استفاده کنند. آگاهی در مورد یک حفره امنیتی همچون اکسپلیوت حتا در یک بازه زمانی کوتاه به کارشناسان امنیتی اجازه می‌دهد اقدامات اولیه را انجام داده، نقاط آسیب‌پذیر را شناسایی و ایزوله کنند تا احتمال نفوذ به ساختار شبکه به حداقل برسد.

انعطاف‌پذیری شبکه‌های ایمن

مجازی‌سازی، رایانش ابری، تحرک‌پذیری، بهینه‌سازی فناوری‌ها، اینترنت اشیا و پیاده‌سازی سامانه‌های هوشمند در بخش تولید باعث شده نگرش سازمان‌ها در ذخیره‌سازی و دسترسی به اطلاعات تغییر اساسی پیدا کند. سازمان‌ها برای مقابله با تهدیدات امنیتی مجبور هستند مکانیزم‌های امنیتی را هم‌طراز با تغییرات دنیای فناوری به‌روز نگه دارند. به‌کارگیری فناوری‌های نوظهوری همچون نرم‌افزار به عنوان سرویس، پلتفرم به عنوان سرویس و زیرساخت به عنوان سرویس، مخاطرات جدیدی به همراه آورده‌اند. تیم‌های امنیت اطلاعات برای محافظت از سامانه‌های قدیمی و درون سازمانی در برابر تهدیدات جدید باید زیرساخت امنیتی سازمان را توسعه و ارتقا دهند. پژوهش‌ها نشان می‌دهند، معماری امنیت اطلاعات مبتنی بر دارایی‌ها (Asset-Based) و محدود به شبکه همانند گذشته اثربخشی چندانی ندارند و قادر نیستند به شکل مطلوبی برای شناسایی ریسک‌ها و آسیب‌پذیری‌ها به کار گرفته شوند. به همین دلیل باید مدل‌های پردازشی قابل اطمینان با هدف کاهش ریسک‌پذیری افشای اطلاعات سازمانی و محافظت از زیرساخت‌های حیاتی بازنگری شوند.
انعطاف‌پذیری سایبری با ارائه چارچوبی قابل اعتماد پاسخی برای مشکلات رایج است. انعطاف‌پذیری سایبری با هدف پیشگیری از خطرات سایبری، سعی می‌کند نفوذ به سازمان را کاهش دهد. محافظت پویا یکی از الگوهای اجرایی انعطاف‌پذیری سایبری است که اجازه می‌دهد زمانی که شبکه سازمان آلوده شده، بازهم خدمت‌رسانی به مشتریان انجام شود. راهکار فوق نیازمند شبکه‌ای هوشمند است که بتواند با اولویت‌بندی ترافیک، هرگونه فعالیت مشکوک را ایزوله و متمایز از شبکه اصلی کند و همزمان امکان مسیردهی مجدد منابع جدید را داشته باشد. یک چنین راهکار کارآمدی در سایه به‌کارگیری معماری‌های ابرمحور پویا که زمان پاسخ‌دهی به کاربران را کاهش می‌دهند، امکان‌پذیر است.

منبع:

cisco
تاریخ انتشار:
19 فروردین 1399

نشانی منبع:
https://www.shabakeh-mag.com/security/16756/%D8%A7%D9%86%D8%B9%D8%B7%D8%A7%D9%81%E2%80%8C%D9%BE%D8%B0%DB%8C%D8%B1%DB%8C-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C-%DA%86%DB%8C%D8%B3%D8%AA-%D9%88-%DA%A9%D8%A7%D8%B1%D8%A8%D8%B1%D8%AF-%D8%A2%D9%86-%D8%AF%D8%B1-%D8%AF%D9%86%DB%8C%D8%A7%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%B3%D8%AA%D8%9F