خطة العمل

أين وصلت مرحلة تنظيم الحماية؟

عند تنصيب برنامج **Security Onion** بعد توصية فريق SEB سيكون بمقدور ال IT الإطلاع على حركة المعلومات الخارجة والواردة من الشبكة مما سيمكنه من تحديد المخاطر او الإختراقات المحتملة داخل الشبكة.

إلى الأن نحن في مرحلة **1** من **3** حيث تم اعداد خادم ال VPNعلى الراوتر في مكتب الفريق في عمان حيث بامكان الموظفين داخل المكتب بالاتصال عن طريق شبكة ال VPN بدون الحاجة لاستعمال برنامج Proton

المرحلة 2: يجب ان نقوم بتنفيذ امكانية الاتصال من خارج شبكة عمان الى شبكة عمان ومن ثم تحويلها الى شبكة VPN

المرحلة 3: جميع هذه الاتصالات من الاجهزة سواء من شبكة عمان او الخارجية سيتم تحويلها الى برنامج **Security Onion** .

ماهي المشاكل التي نواجهها في هذا الإعداد وحلولها؟

حسب عدة تجارب واختبارات وبتنسيق مع H2A تبين أن الراوتر الحالي لا يدعم المرحلة الثانية حيث انه يدعم تقنية Client-To-Site VPN فقط والمطلوب هو Site-to-Site VPN
اي انه يدعم اتصال VPN من الراوتر فقط وليس اتصال VPN ان كان المتصل من خارج الشبكة.

الحل المنطقي: أعتقد أننا بحاجة إلى استبدال جهاز التوجيه بجهاز يدعم هذه ميزة Site-to-Site VPN

الحل الأخر **غير منطقي**: أن يقوم المستخدمون من هم خارج مكتب عمان بالاتصال عبر تطبيق Proton بعد استخدام OpenVPN، لكن هذه الخطوة مزعجة لحد ما.

سيتم البحث عن النوع المحدد من الراوترات لانتقاء الأفضل والذي يلبي احتياجات المرحلة.
حسب بحثي الاولي فأن جهاز Asus RT-AX88U قد يكون ملائم لهذا الغرض وسأناقش ذلك من James

المراسلات عبر الايميلات التي تم تخصيصها في Proton:

في نوفمبر 2024 تم ارسال دعوات عبر البريد الالكتروني للأشخاص الموجودين في جدول ايتانا والموضوعين ضمن الأولوية 1 للبدء بإستعمال الايميلات المربوطة بالدومين etanasy.org و etana-drt.org، تم قبول الدعوات عبر الايميل من الفريق بإستثناء (Alaa و Tom و Zenobia).

إلى الأن يبدو ان الفريق لا يعتمد على Proton بإستثناء (Tareq و Issam و Raed) استناداً الى المساحات المشغولة ضمن مخصصاتهم.

سأقدم الدعم المطلوب واقتراحات حماية للإيميلات في هذه المرحلة لضمان الانتقال السلس من الايميلات القديمة الى Proton. وذلك حسب سبب امتناع كل شخص.

التوصيات المقترحة من قبل H2A

كافة النصائح التي تم تقديمها من قبل H2A ذات قيمة صحية وسليمة بدءاً من استعمال VPN وبرامج المصادقة والانتباه للروابط وطريقة حفظ البيانات واستعمال كلمات سر قوية وصولاً لاستعمال Faraday Bags للهواتف والاجهزة المحمولة إلا انني لا أرى ان حمل **"Faraday Bag"** ضرورياً دائماً إلا أثناء السفر او حضور الاجتماعات.

استكمالاً لذلك لم يكن هناك ترشيح من قبل H2A لنقطة هامة لبرامج حماية

على سبيل المثال ارشح بشكل شخصي Avast/ComodoFirewall/Avira، ربما هذا الأمر يعتمد على مواصفات كل جهاز على حدى.

جلسة مناقشة مفتوحة مع كل موظف

إعداد المواعيد وتخصيص جلسة لكل موظف: استخدام Google Calendar لتحديد مواعيد منظمة مع كل عضو من الفريق مع مراعاة الوقت المناسب.

إرسال نموذج لجمع البيانات حول الأجهزة المستخدمة، مثل أنظمة التشغيل والبرامج. رابط النموذج، سيتم ارساله بشكل فردي لكل موظف في الفريق قبل بدء الجلسة.

الهدف من الجلسة: الجلسة غايتها الاساسية فهم طبيعة الحماية الرقمية المتبعة من كل موظف في الفريق وتفهُم مخاوفه الأمنية في استخدام الانترنت وارشاده نحو طرق أمنة، ايضاً يتم تقييم مدى التزام الفريق بالأمن السيبراني

يتم إجراء التقييم الدوري كل **3-6 أشهر** حسب الحاجة ومستوى المخاطر المحددة.

أساليب وأدوات سيكون الفريق مُلزم بتنفيذها لضمان الحماية:

1. عند القيام بالاتصال او التصفح الى قاعدة البيانات يجب ان يكون الاتصال بالـ VPN المحدد.
2. يجب ضمان استعمال كلمات سر قوية محفوظة بشكل أمن.
3. يجب تفعيل ميزة التحقق بخطوتين عن طريق برامج التحقق مثل Google authenticator.
4. يجب ضمان وجود برنامج AntiVirus واحد على الأقل.
5. التأكد من التزام الموظف بإستعمال برامج المحادثة المشفرة مثل Signal.

تنويه: للأشخاص الذي يرغبون زيارة سوريا تم التأكد أن برنامج Proton VPN يعمل بشكل جيد في سوريا بدون مشاكل

الخطط المستقبلية

- في حال انتقال إيتانا للداخل السوري (الدخول والخروج المتكرر) أرغب بطرح فكرة لحماية البيانات من الدخول أو الاطلاع عليها خصوصاً فيزيائياً في ظل عدم وضوح الرؤية للإدارة الجديدة في سوريا. مثال (هل سيكون هناك تدقيق على محتوى اجهزة اللاب توب او اقراص التخزين؟)

  هذه النقطة ماتزال شائكة لكن أرغب فعلياً في طرح تقنية تُدعى **Disk encryption** وأفضل البرامج المتاحة لذلك هي **VeraCrypt**.

  ما هو برنامج **VeraCrypt**؟
  هو برنامج يُمكن المستخدم من إنشاء قرص افتراضي مشفر يعمل تمامًا مثل قرص عادي ولكن داخل ملف وبمساحة معينة لإخفاءه عن الظهور ضمن اقراص جهاز الكمبيوتر.

- سأبقى على الاطلاع بأحدث أساليب الإختراق المتبعة والتحذير منها وارسال تنبيهات للفريق في حال وجود اي تغيير طارئ او مشاكل محتملة.

الختام

قد تبدو خطوات الحماية معقدة لبعض الموظفين لكن مع ازدياد كثافة المعلومات والانتشار الإعلامي تُصبح اي مؤسسة هدف للاختراق والعبث، هدفي في الجانب التقني زيادة الوعي والتعاون لنُصبح أكثر سلامة واطمئنان وتجنب اي مخاطر قد تضر في سير العمل.