نقطة
nuqta

القرصنة الإلكترونية

في افريقيا

nuqtaDoc

مع دخولها ساحة الرقمنة هل تقف إفريقيا في مرمى القرصنة الإلكترونية؟

في طريقها نحو الرقمنة الشاملة، تواجه إفريقيا زيادة ملحوظة في نشـــــــاط الجريمة الإلكترونية. ومن المتوقع أن يصل الاقتصاد الإلكتروني في إفريقيا إلى 180 مليار دولار سنويًّا بحلول عام 2025. إذ يوفر القطاع الرقمي المزدهر في إفريقيا فرصة لبدء الحكومات دورة نمو جديدة في أعقاب جائحة كوفيد، وذلك من خلال نشر التقنيات الرقمية والبيانات والربط بين جميع القطاعات، لكن الجهود غير الكافية في القارة لمنع الجرائم الإلكترونية يمكن أن تعرقل هذا النمو.

في النصف الأول من عام 2020 وحده، كانت إفريقيا هدفا لـ28 مليون هجوم إلكتروني تسببت في خسائر تقدر بنحو 4 مليارات دولار. أكثر من 85% من المؤسسات المالية تؤكد أنها عانت من هذا النوع من الهجوم.

ستحتاج الحكومات والشركات الإفريقية إلى الاستثمار بشكل كبير في الأمن الرقمي، حيث تمثل الهجمات الإلكترونية تهديدًا أكبر للمنطقة التي تتضاعف فيها حركة الإنترنت كل 18 شهرًا.

سرعة انتشار خدمات الإنترنت في إفريـقيا:

495 مليون

شخص في إفريقيا جنوب الصحراء اشتركوا في خدمات الهاتف المحمول.

46%

من سكان المنطقة أصبحوا متصلين بالإنترنت بزيادة قدرها 20 مليوناً وفقًا لاتحاد الاتصالات السلكية واللاسلكية.

303 مليون

شخص في المنطقة متصلون بالإنترنت عبر الهاتف المحمول.

621 مليون

دولار قيمة محافظ النقود المحمولة المسجلة.

39% -17%

زيادة في التعاملات المالية عبر الإنترنت في 2021 لتصل إلى 701.4 مليار دولار.

من المتوقع أن يرتفع عدد مستخدمي الإنترنت في إفريقيا بنسبة 11%، ما يمثل 16% من إجمالي المبلغ العالمي وفقًا لمؤسسة التمويل الدولية (IFC)، وهي تتبع البنك الدولي. إضافةً إلى ذلك بدأ الأفارقة بالفعل الانتقال من شبكة 3G إلى 4G:

عام 2020 كانت شبكة 4G تمثل 12% فقط من اتصالات الهاتف المحمول في القارة، ولكن من المتوقع أن تتجاوز 28% بحلول عام 2025. تشير الأبحاث إلى أنه من المتوقع مساهمة الاقتصاد الإلكتروني في إفريقيا بمبلغ 180 مليار دولار في الاقتصاد الكلي بحلول عام 2025، وأن يرتفع إلى 712 مليار دولار بحلول عام 2050.

ومع ذلك، فإن هذه الرقمنة السريعة تخلق التهديدات كما تخلق الفرص. إذ إن ما يقرب من 90% من الشركات الإفريقية تعمل من دون بروتوكولات الأمن السيبراني اللازمة.

تكلـــــفـــــــة
جرائم الإنترنت:

إفريقـيا: 4 مليـــــــارات دولار

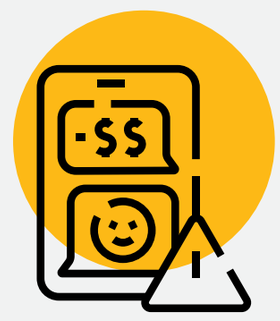
جنوب إفريقـيـا: 570 مليون دولار

نيجيريا: 500 مليـــــــون دولار

كينيا: 36 مليـــــــــون دولار

تشمل التهديدات السيبرانية في إفريقيا:

عمليات الاحتيال عبر الإنترنت



الابتزاز الرقمي

توزيع البرامج الضارة

اختراق البريد الإلكتروني للشركات

برامج الفدية الخبيثة (وهو برنامج ضار مصمم لمنع وصول مستخدم أو مؤسسة إلى الملفات الموجودة على أجهزة الكمبيوتر الخاصة بهم، وذلك من خلال تشفير هذه الملفات والمطالبة بدفع فدية لمفتاح فك التشفير).

شبكات الروبوت.

التصيد الاحتيالي (رسائل البريد الإلكتروني المرسلة بقصد خداع الأشخاص للكشف عن معلوماتهم الشخصية).

يبلغ عدد عمليات الكشف عن ضحايا القرصنة الإلكترونية في إفريقيا حوالي 3900 عملية شهريًّا، وذلك وفقًا للإنتربول.

TREND MICRO™

سجلت شركة "Trend Micro"، وهي شركة برمجيات إلكترونية يابانية، عددًا كبيرًا من التهديدات في إفريقيا منذ يناير 2020 حتى فبراير 2021 موزعة كالتالي:

679 مليون
اكتشاف عبر البريد الإلكتروني

8.2 مليون
اكتشاف في الملفات

14.3 مليون
اكتشاف على شبكة الويب

وجدت دراسة أجرتها شركة "Deloitte"، عام 2021، أن 40% من الشركات الإفريقية سجلت عددًا متزايدًا من الحوادث السيبرانية بين عامي 2020 و2022.
وقفزت هجمات البرمجيات الخبيثة في جنوب إفريقيا بنسبة 22% في الربع الأول من عام 2019 مقارنة بالفترة نفسها من عام 2018، أي ما يقل عن 577 محاولة هجوم في الساعة، وذلك وفقًا لشركة كاسبرسكي للأمن السيبراني.

الهواتف المحمولة التي تعمل بنظام أندرويد في جنوب إفريقيا احتلت المرتبة الثانية من حيث استهداف البرامج الضارة المصرفية في جميع أنحاء العالم بعد روسيا. وتشير التقديرات إلى أن واحدًا من كل تسعة هواتف محمولة تعمل بنظام أندرويد في نيجيريا لديه تطبيقات مصابة بالبرامج الضارة.

أكثر الهجمات السيبرانية تأثيرًا في إفريقيا

برامج الفدية الخبيثة

هاجمت أكثر من أكثر من

%61

من الشركات في جميع أنحاء إفريقيا.

الاحتيال على بطاقات الائتمان

يمثل

%79.5

من خسائر الاقتصاد في عدد من الدول أبرزها جنوب إفريقيا.

مع تصاعد الهجمات الإلكترونية على البنية التحتية البحرية، والتي تتراوح بين القرصنة وسرقة سجلات المعاملات، يخشى الخبراء أن تكون الموانئ الإفريقية وصناعات الشحن هي الهدف المقبل.

في المقابل بلغت قيمة سوق الأمن السيبراني في إفريقيا 2.5 مليار دولار عام 2020 ، وذلك وفقًا لشركات الأبحاث التسويقية. وتعد الدول الإفريقية الأقل التزامًا بالأمن السيبراني في العالم:

عدد متخصصي الأمن المعتمدين في عام 2018 بلغ

7000 شخص فقط

ما يمثل واحدًا لكل

185000 شخص

يبلغ العجز في القارة

100000 شخص

في المتخصصين المعتمدين بمجال الأمن السيبراني.

أبرز الحوادث السيبرانية 2020 - 2022

يستهدف مجرمو الإنترنت قطاعي البنوك والرعاية الصحية الخاصة في إفريقيا. وكانت البلدان الإفريقية هي الهدف المفضل لعصابات مجرمي الإنترنت الدوليين، ويرجع ذلك جزئيًّا إلى دفاعاتهم الإلكترونية الضعيفة.

أوائل أكتوبر 2020، واجه قطاعا الاتصالات والبنوك في أوغندا أزمة عقب اختراق كبير لشبكة الأموال عبر الهاتف المحمول في البلاد. استخدم المتسللون حوالي 2000 بطاقة SIM للهاتف المحمول للوصول إلى النظام، وتم سرقة ما يقدر بنحو 3.2 ملايين دولار.

في يونيو 2020، تعرضت شركة "Life Healthcare"، ثاني أكبر مشغل للمستشفيات في جنوب إفريقيا، لهجوم إلكتروني في منتصف جائحة كوفيد، ما أدى إلى تعطيل مزود 6500 سرير وإجباره على التحول إلى أنظمة النسخ الاحتياطي اليدوية.

يشير بعض المحللين بأصابع الاتهام إلى عصابات دولية يمكن إدارتها من البرازيل وروسيا والصين وبعض البلدان الإفريقية كنيجيريا وجنوب إفريقيا.

مأزق البنوك الإفريقية

وفقًا لشركة "Dataprotect"، وهي شركة أمن بيانات مقرها المغرب، فإن البنوك الإفريقية جنوب الصحراء معرضة بشكل خاص للهجمات الإلكترونية، ويرجع ذلك أساسًا إلى قلة الفنيين المؤهلين ونقص الاستثمار في الأمن السيبراني:

أكثر من 85% وقعوا بالفعل ضحية هجوم إلكتروني واحد على الأقل.
30% من الهجمات احتيال بالبطاقات المصرفية.
33% عمليات تصيد احتيالي.

24% من الهجمات كانت على البنوك الكبرى في إفريقيا، بما في ذلك الفيروسات والاختراقات التي أثرت في أنظمة المعلومات. إضافةً إلى ذلك تتأثر البنوك بنمط محدد من الهجمات منها:

تسريب المعلومات
سرقة الهوية
الاحتيال في تحويل الأموال
عمليات الاحتيال المزيفة عن طريق الشيكات.

أكثـــــر الدول تأثرًا بعمـــليات اختراق البريد الالكتـروني:

جنوب إفريقيا 34%

تونـــــــــس 20%

المغـــــــرب 12%

موريشيـوس 12%

نيـجـيـــــريا 11%

كيـــــنـــــيا 9%

أبرز البلدان التي تنطلق منها الهجمات السيبرانية في إفريقيا:

نيجيريا 83%

جنوب إفريقيا 14%

غانا 10%

الصنـــاعات الأكثر تضررًا في إفريقيا:

القطاع الحكومي
قطاع الأغذية والمشروبات
قطاع التصنيع
القطاع المصرفي

المواجهة القانونية:

وقّعت 13 دولة إفريقية على اتفاقية الأمن السيبراني. حدد الاتحاد الإفريقي إطار عمل للأمن السـيبراني في إفريقيـا لتنظيـم المعامـلات الإلكترونيـة وحمـاية البيانـات الشـخصية وتعزيـز الأمـن السـيبراني والحوكمة الإلكترونية ومكافحة الجريمة السيبرانية. بحلـول مايو 2022، صدَّق على الاتفاقية 13 من 55 دولة عضـو فـي الاتحاد الإفريقـي (أنغولا والـرأس الأخضر وغانـا وغينيـا وموريشـيوس وموزمبيـق وناميبيـا والنيجر وجمهورية الكونغو ورواندا والسنغال وتوغو وزامبيـا). وفـي الشـهر نفسـه، كانـت ثمانـي دول إفريقيـة فقـط لديهـا اسـتراتيجيات وطنيـة للأمـن السيبراني.

مـع وجود حوالي 41% من سـكان المنطقة دون سـن 15 عامًـا، فإن 120 مليون مسـتهلك جديـد من الشـباب الإفريقي سـيمتلكون هاتفًا جـوالًا للمرة الأولى خلال السـنوات القليلة المقبلة، وسيشـاركون في الاقتصاد الرقمي، ما يشـير إلـى ضرورة امتلاك القارة دفاعات إلكترونية ضخمة ضد الهجمات السـيبرانية التي تزداد وتيرتها كلما زاد استخدام الإنترنت.

أهـم البـــــلدان التي تتـــــبـــنى الأمن السيبراني في إفريـــقـــــيا:

أبيدجان

توغو

مالي

النيجر

بوركينا فاسو

حيـث ســرقت مجموعــة قرصنة 11 مليـون دولار من الدول الســالف ذكرها عــن طريق 30 هجومًا ناجحًــا ضد البنــوك ومقدمـي الخدمـــــــــات المالية وشركات الاتصالات.

أكـــثـــــر البـــلدان تضررًا من الهـجـمات السيبرانية في إفريقيا بين 2018 و2022

كوت ديفوار

مالي

بوركينا فاسو

بنين

الكاميرون

الجابون

النيجر

نيجيريا

السنغال

سيراليون

توغو

أوغندا

حيـث سـرقت مجموعـة قرصنة 11 مليـون دولار من الدول السـالف ذكرها عـن طريق 30 هجومًا ناجحًـا ضد البنـوك ومقدمـي الخدمـــــــات المالية وشركات الاتصالات.

تأثير التهديدات الإلكترونية في الاقتصـــــاد الإفريقي:

خفضت الجريمة السـيبرانية الناتج المحلي الإجمالي في إفريقيا بأكثر من 10%، بتكلفة تقدر بنحو 4.12 مليار دولار أمريكي في عام 2021.

زادت نسـبة الهجمـات الإلكترونيـة ضـد منصـات الخدمـات المصرفيـة عبـر الإنترنـت منـذ عـام 2020 بنسبة 238%.

وفقًـا لمركز معلومات المخاطـر المصرفية في جنوب إفريقيا، تخسـر جنوب إفريقيا 157 مليون دولار سنويًا بسبب الهجمات الإلكترونية.

أتاح التوسـع في منصات الاتصال عبر الإنترنت بيئة تعليمية لمجرمـي الإنترنت لتطوير مهاراتهم وتعزيزها، وتعلم وتبادل المعلومات حول مجموعات أدوات الجرائم الإلكترونية، وحتى تبادل الدروس المسـتفادة، والبيانات المسروقة، وعمليات الاستغلال الناجحة مع أفراد آخرين.

يقـوم مجرمو الإنترنـت بتجنيد أعضاء جدد مـن خلال التدريب وتقديم عدد من أدوات الجرائم الإلكترونية.
كان هذا أحد أسباب توسع عمليات "DDoS" في هذا النوع من الجرائـم الإلكترونيـة كخدمة متاحة من خـلال الويب المفتوح والمظلم.

يـزداد التحـدي السـيبراني فـي إفريقيـا. فبحلـول عـام 2030 سيكون إنترنت الأشياء سـوقًا ضخمة في المنطقة، وحينها سـيتصل نحو عشـرة مليارات جهـاز بالإنترنت، بمـا في ذلك السيارات والكاميرات وأجهزة الاستشعار وأجهزة الكمبيوتر المحمولة وجميع المعاملات المالية.

وفـي عصـر الرقمنـة وإنترنـت الأشـياء، يحيـط التهديـد السـيبراني بالقـارة السـمراء بشـكل مقلـق، وعليـه تحتـاج المؤسسـات والحكومات الإفريقيـة إلى تكثيف جهودها قبل أن تسيطر العصابات غير المرئية على مصير القارة بأسرها.

شكراً