METROBANK

Resumen Reportes de Operaciones e Inteligencia 2018

Julio 31, 2018

Este reporte complementa y resume la información detallada de los reportes mensuales técnicos y ejecutivos presentados a METROBANK a través de nuestra plataforma de gestión GMP en lo que va el año 2018.

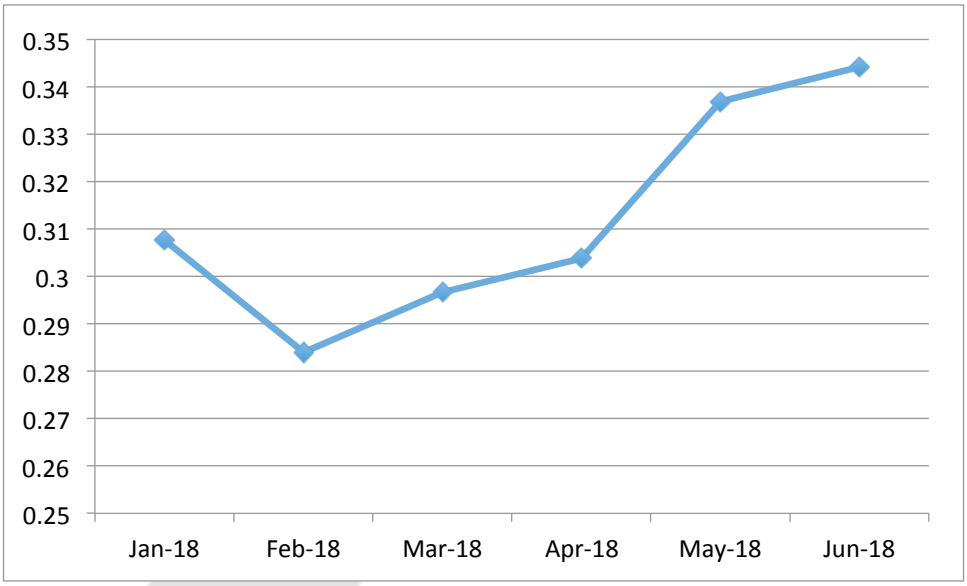
Estado de Seguridad

De acuerdo al modelo de GLESEC de los Siete Elementos (**7eCSM™**) presentamos el estado de seguridad de la organización agrupado por cada "elemento" de nuestro modelo.

Riesgo

El METROBANK presenta riesgos de seguridad que se están incrementando como se puede observar en la información indicada más abajo.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



Hay que considerar lo siguiente:

Los factores de riesgo se basan en información de los servicios de gestión de vulnerabilidad y del servicio de simulación de brechas de seguridad. Este ultimo no ha sido adquirido y no esta en operación. Se recomienda realizar la prueba de concepto del mismo (MSS-BAS POC). Se puede observar que el factor de riesgo se encuentra en crecimiento por los últimos cinco meses en base a las condiciones de vulnerabilidades.

También es importante destacar que en este momento no se esta testeando las vulnerabilidades internas. Si consideramos las vulnerabilidades internas como reflejo de las externas y dado la gran cantidad de sistemas internos (respecto al perímetro) se asume que los hallazgos de vulnerabilidades serán también significativos. El no testearlo no implica que no haya riesgo.

Vulnerabilidad

La organización presenta un muy alto grado de vulnerabilidades (10 de los 13 sistemas en el perímetro tienen vulnerabilidades) y entre criticas y altas hay 12 vulnerabilidades las cuales si son explotadas pueden producir daño a METROBANK. Estas vulnerabilidades han sido reportadas en los Reportes de Incidentes y en los “Reportes Mensuales de Operaciones e Inteligencia” con recomendación de remediación a ser aplicadas. Abajo se

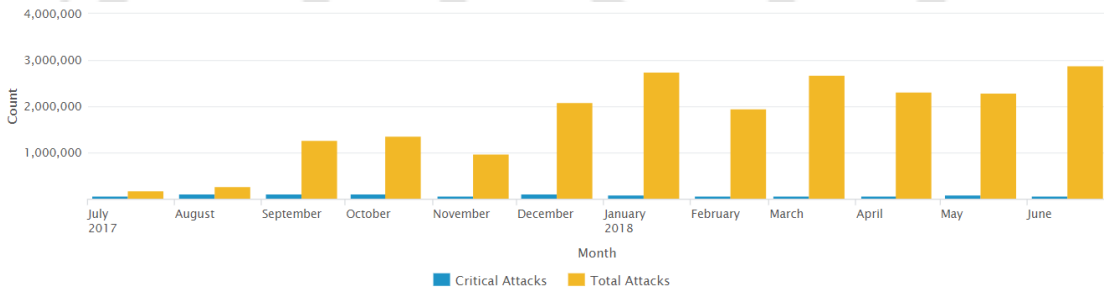
ve la tabla del mismo.

EXTERNAL	Jan-18	Feb-18	Mar-18	Apr-18	May-18	Jun-18
Total Number of Systems:	9	14	13	14	13	13
Total Number of Systems Vulnerable:	*7*	*10*	*10*	*11*	*11*	*10*
Total Number of Critical Vulnerabilities:	0	0	0	0	1	1
Total Number of High Vulnerabilities:	0	1	0	0	0	11
Total Number of Medium Vulnerabilities:	34	46	40	43	38	32
Total Number of Low Vulnerabilities:	12	17	16	17	15	16
Total Number of Vulnerabilities:	*46*	*64*	*56*	*60*	*54*	*60*
Risk Value Metric Factor	*0.3077*	*0.284*	*0.2967*	*0.3038*	*0.3369*	*0.3442*

Nuevamente llamamos la atención a que solo vemos las vulnerabilidades externas y si fuéramos a testear las internas nos podríamos encontrar con un tema importante de remediación.

Amenazas

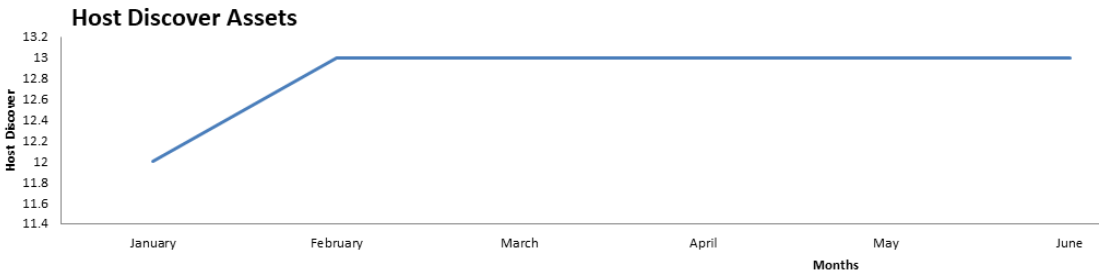
Nuestra visibilidad de amenazas de la organización es limitada y se basa en el servicio MSS-APS y MSS-APFW. Aun así, el crecimiento de ataques de este año comparado al 2017 es muy significativo. Consideramos muy importante el ampliar la visibilidad y considerar otras fuentes de amenazas como las que provee el MSS-SIEM (con información de los firewalls y otros sistemas) y el MSS-EIR (actividad sospechosa en las estaciones de trabajo y servidores).



Activos

“No se puede proteger lo que no se conoce”

Como solo se tiene visibilidad externa y hay pocos sistemas en el perímetro representamos esto en la grafica que sigue. La cantidad de sistemas se mantiene constante.



La identificación de activos aplicativos no se puede realizar ya que este servicio (MSS-EPS) no esta contratado.

Cumplimiento

Servicio MSS-EPS no contratado.

Validación

Servicio MSS-BAS no contratado.

Acceso

No se tiene información relacionada con quien accede a los sistemas críticos del METROBANK. Esta información la pueden proveer los servicios MSS-TAS y MSS-PIM (ambos no contratados).

Estado de Servicios Contratados

Servicio	Descripción	Estatus	Expiración
MSS-APS	Servicio de Protección contra ataques de Denegación de Servicio e intrusos	Activo	Junio 30, 2019
MSS-APFW	Servicio de Protección contra ataques a nivel aplicativos	Activo	Junio 30, 2019
MSS-VME	Servicio de descubrimiento de activos de red en el perímetro y testeo de vulnerabilidades en el perímetro (cloud)	Activo	Junio 30, 2019
MSS-VMI	Servicio de descubrimiento de activos internos de red y testeo de vulnerabilidades interno (GMSA)	No activo	n/a
MSS-EPS	Servicio de descubrimiento de activos aplicativos, de todos los sistemas (estaciones de trabajo y servidores) y monitoreo de desviaciones a cumplimiento (GMSA)	No activo	n/a
MSS-SIEM	Servicio de correlación de eventos de seguridad y manejo de incidentes (GMSA)	No activo	n/a

MSS-EIR	Servicio de detección de actividad sospechosa, malware y Ransomware, contención, protección e investigación.	No activo	n/a

Comentarios y Recomendaciones

Se ha avanzado mucho en el fortalecimiento de la seguridad informática de METROBANK. Lo primero fue crear conciencia obteniendo visibilidad de una cantidad de elementos y a través de un portal que hoy consolida la información a nivel ejecutivo y táctico como lo es el portal GMP. También se destaca la buena colaboración con los equipos de trabajo.

Consideramos las siguientes recomendaciones de mejora:

Establecer una mejora en la forma de operar entre el METROBANK y GLESEC de tal manera que aumentemos la efectividad de nuestros esfuerzos combinados. Concretamente proponemos el utilizar nuestro sistema de tickets y que el personal de GLESEC aborde los temas que el METROBANK no este preparado o no tenga tiempo para abordar. Esto implica el agregar horas de consultoría mensual de servicios profesionales. También proponemos una reunión mensual en-sitio del personal de servicios profesionales de GLESEC para efectos de coordinación y trabajo de remediación con el personal técnico del METROBANK. Estas acciones, que la Gerencia de Informática y la Vicepresidencia podrá monitorear en el GMP y en los Reportes Mensuales de Operaciones e Inteligencia debería producir una reducción sistemática de vulnerabilidades y condiciones de riesgo del banco.

Hay varias otros servicios de gran importancia a considerar para el METROBANK, estos son: Gestión de Brechas de Seguridad (MSS-BAS); Correlación y manejo de incidentes (MSS-SIEM); Identificación de actividad sospechosa y protección de servidores y estaciones de trabajo (MSS-EIR) y Gestión de Cuentas Privilegiadas (MSS-PIM).

Recomendaciones en una lista:

1. Utilizar el Sistema de Tickets de GLESEC (portal GMP) para todos los temas de seguridad informática por parte del personal de GLESEC y del METROBANK
2. Asignación de tickets entre GLESEC y el METROBANK de tal manera de trabajar en conjunto en la mitigación
3. Programación de reunión mensual de Servicios Profesionales en el METROBANK para efectos de coordinación
4. Considerar agregar horas mensuales al contrato para poder colaborar mas activamente en los temas de remediación.

5. Considerar el agregar el servicio MSS-SIEM para la captura de datos de los Firewalls de Check Point, correlación de la información y gestión de incidentes.
6. Proveer acceso a la Vicepresidencia de Informática del METROBANK y a otras áreas como lo consideren al portal GMP en el "rol" correspondiente.
7. Realizar prueba de concepto del servicio de gestión de brechas simuladas (MSS-BAS POC).
8. Consideración de adquisición de los siguientes servicios:
    a. Gestión de Brechas de Seguridad (MSS-BAS),
    b. Gestión de Correlación y Manejo de Incidentes (MSS-SIEM),
    c. Servicio de gestión de vulnerabilidad interna (MSS-VMI),
    d. Servicio de gestión de acceso con doble factor de autenticación (MSS-TAS),
    e. Identificación de actividad sospechosa y protección de servidores y estaciones de trabajo (MSS-EIR) y
    f. Gestión de Cuentas Privilegiadas (MSS-PIM).

De lo recomendado arriba una forma efectiva de proceder es de completar los siete elementos (7eCSM™) a nivel de perímetro con servicios CLOUD como ser:

MSS-SIEM (Check Point y sistema de anti-virus; estimado 1GB/indexación por día).

MSS-TAS *

MSS-EIR *

MSS-EPS *

*: dimensionado para los servidores del perímetro – 13

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355