MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Protocollo Sisifo: **96A283F2DE**

Siena, 30/08/2018

FUNZIONI COMPILATRICI:
Amministratore Delegato - MPS

Comunicazione per:
Consiglio Di Amministrazione - MPS

OGGETTO:

Aggiornamento sulla parziale interruzione di servizio ATM del 19.02.2018

Indice degli allegati:

- *Allegato 1 – Relazione Direzione Chief Audit Executive su incidente ATM*
- *Allegato 2 – Accordo commerciale per MPS – modulo base*

1. MOTIVAZIONE

Aggiornare il Consiglio di Amministrazione sulle azioni messe in atto a seguito dell'incidente del 19 febbraio che, come già rappresentato nella seduta del CDA del 1 marzo 2018, ha comportato l'interruzione del servizio su un lotto di circa 500 ATM.

2. INFORMAZIONI RILEVANTI

- Il 19 febbraio 2018 un errore commesso da un collaboratore della società FabbricaDigitale s.r.l., sub-fornitore della società Bassilichi S.p.A. del Gruppo Nexi, ha potenzialmente compromesso il funzionamento di 1.456 ATM su 2.758.
- Le azioni di rimedio messe subito in atto hanno consentito di limitare il disservizio a 499 ATM (18% del parco attivo) con un picco massimo giornaliero di 430 ATM bloccati.
- L'incidente è stato contestato alla società Bassilichi, appartenente al Gruppo Nexi, con una lettera inviata il 23 febbraio a firma congiunta del Consorzio Operativo Gruppo Montepaschi (nel seguito "COG") e della Banca Monte dei Paschi di Siena (nel seguito "BMPS").
- La presente comunicazione fornisce un aggiornamento sull'evoluzione dei rapporti commerciali con il Gruppo Nexi e sulle azioni messe in atto per evitare il ripetersi di quanto accaduto sugli ATM e, più in generale, per rafforzare la sicurezza informatica del Gruppo MPS.

2.1 DESCRIZIONE INCIDENTE

Come già rappresentato nella seduta del CDA del 1 marzo 2018, al momento dell'incidente il parco ATM di BMPS era costituito da 2.758 dispositivi[1]. In tali apparati è presente "*Digital Signage*", un

[1] Nel frattempo sono intervenute nuove installazioni che hanno elevato il parco a 2801 unità.

software che permette di distribuire e pubblicare contenuti pubblicitari secondo determinati palinsesti.

Digital Signage è sviluppato con l'uso di Xuniplay prodotto dalla società FabbricaDigitale s.r.l. acquisito dal COG per mezzo di un contratto stipulato tra COG e Bassilichi S.p.A. in qualità di *Prime Contractor.* Tale contratto disciplina (tra le altre condizioni) le modalità di manutenzione: aggiornamento, gestione sistemistica, etc.

La suite Xuniplay è un sistema complesso in grado di trasferire contenuti da un server centrale alle macchine ATM, Monitor e Tablet per la firma grafometrica ubicate in periferia e di eseguire da remoto attività di manutenzione di tutti gli elementi della suite Xuniplay.

Il giorno 19 febbraio 2018, alle ore 9:35, un collaboratore della società FabbricaDigitale s.r.l., sub-fornitore della società Bassilichi S.p.A., ha avviato una procedura di pulizia e cancellazione di file *Digital Signage,* non più necessari, dalle macchine ATM. Questa attività non era stata autorizzata da alcuna funzione COG.

Tale intervento ha provocato la cancellazione di tutti i file di Sistema Operativo su 1.456 ATM. Per conseguenza le macchine ATM di questo gruppo, pur continuando ad essere operative, non erano più in grado di ritornare in attività nel caso in cui per una qualsiasi ragione (indotta o casuale) avessero ricevuto un comando di spegnimento e riavvio.

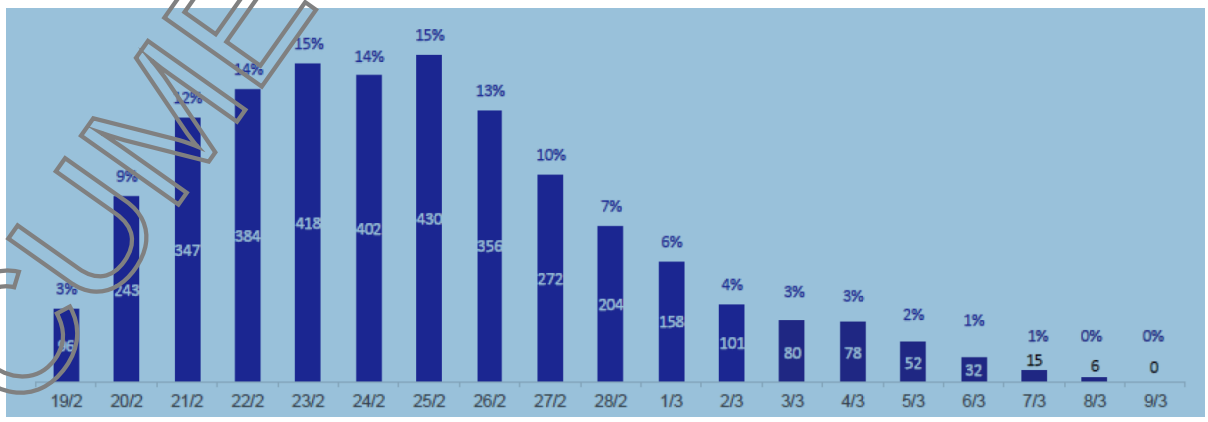
Sono state avviate le procedure previste in caso di grave incidente e contestualmente: è stato disattivato "*Digital Signage*", è stata inibita ogni forma di spegnimento programmato degli ATM impattati ed è stata avviata una task force coordinata dalla struttura ATM Manager di BMPS per gestire le necessarie azioni di recupero.

Azioni di recupero:

a) messaggio in bacheca con cui si invitavano le filiali a non riavviare gli apparati;
b) attivazione di una procedura ad hoc che evitava lo spegnimento del parco macchine da bonificare;
c) bonifica da remoto degli ATM ancora in funzione;
d) ripristino on site degli ATM colpiti da interruzione del servizio.

Grazie alle attività della Task force, gli effetti del disservizio sono stati rimossi, limitando il numero degli ATM fuori servizio ad un massimo di 430 nella giornata del 25 febbraio.

Fig. 1 - Dinamica degli atm inattivi a causa dell'incidente



Per approfondire le cause dell'incidente e la dinamica degli eventi, la Direzione Chief Audit Executive di Capogruppo ha condotto uno specifico approfondimento nell'ambito della revisione ordinaria sulla gestione degli ATM, prevista dal Piano di Audit 2018 e già avviata al momento dell'incidente.

I risultati dell'approfondimento sono stati rappresentati alla Direzione del Consorzio il 24/4/2018 e sono stati poi formalizzati in una relazione *(cfr. allegato 1),* presentata al Collegio Sindacale e al Comitato Rischi BMPS il 9/5/2018 e al Comitato dei Consorziati COG del 15/5/2018.

2.2 AZIONI A TUTELA DEL COG E DI BMPS

Il 23 febbraio scorso il COG e BMPS hanno inviato a firma congiunta una lettera di contestazione e reclamo a Bassilichi S.p.A. e per conoscenza a Fabbrica Digitale s.r.l. e Nexi S.p.A., nella quale è stato stigmatizzato il grave comportamento del fornitore e le conseguenze prodotte. Nella stessa lettera, ci si è inoltre riservati, senza limiti di responsabilità, di chiedere il risarcimento di eventuali danni materiali, da perdite commerciali e reputazionali.

Bassilichi ha risposto alla lettera il 28 febbraio in modo interlocutorio scrivendo di aver avviato una verifica sulle cause dell'evento per identificare le diverse responsabilità di tutte le parti coinvolte.

Successivamente allo scambio epistolare ci sono stati diversi incontri di approfondimento sui fatti accaduti nel corso dei quali, oltre a rappresentare al fornitore che tutti i costi sostenuti direttamente da Bassilichi per la risoluzione del problema non avrebbero dovuto in nessun modo essere ribaltati al Gruppo MPS, è stato chiesto il rimborso dei danni, informalmente quantificati in Euro 344.673,00 Euro, oltre ad IVA ove applicabile. La stima dei danni è il risultato della somma di:

- Euro 283.242,00 per minori introiti commissionali di BMPS nel periodo del disservizio;
- Euro 33.388,00 per spese sostenute da BMPS a favore dell'impresa BTV S.p.A. incaricata delle attività di sorveglianza alle operazioni di ripristino;
- Euro 28.043,00 a titolo di risarcimento dei costi del personale interno sostenuti da BMPS e dal COG (risp.: Euro 15.390,00 e Euro 12.653,00) per le attività di ripristino.

Gestione della relazione con Nexi

Per superare quanto accaduto, e nell'ottica di rendere più sicura e robusta la relazione con il gruppo Nexi, è stato concordato il seguente piano di ristoro ed evoluzione della relazione commerciale:

1. Nexi e Bassilichi hanno concordato sul fatto che l'evento trovi origine da attività, errate e non richieste, poste in essere da personale di Fabbrica Digitale, in qualità di subfornitore della Bassilichi S.p.A.
2. Nexi e Bassilichi hanno accettato di non ribaltare su BMPS alcun costo relativo alle attività di ripristino degli ATM in conseguenza dell'incidente.

3. Nexi e BMPS hanno concordato un piano di incentivi commerciali per un controvalore pari a 350k da riconoscere a BMPS nel 2018 (pari all'importo degli impatti subiti dal gruppo MPS) *(cfr. allegato 2).*
4. BMPS e il Consorzio hanno rinunciato a qualsiasi altra richiesta in merito all'accaduto.

Per evitare il ripetersi dell'incidente, è stato inoltre concordato con Nexi e Bassilichi il seguente piano di lavoro per adeguare il prodotto Digital Signage agli standard di Sicurezza del Consorzio senza alcun costo per COG e/o BMPS:

- disattivazione di tutti i moduli/processi non utilizzati e non specificamente necessari a Digital Signage;
- revisione dei controlli di accesso alla consolle di amministrazione di Xuniplay;
- definitiva rimozione di tutte le funzionalità di auto aggiornamento, riconducendo così ogni tipo di modifica e distribuzione agli standard previsti per il processo di Change Management del COG;
- eliminazione, per i moduli/processi in essere, delle prerogative di amministratore di sistema che hanno permesso la cancellazione dei file di sistema;
- divisione tra i vari pacchetti applicativi che compongono il prodotto, in modo da frazionare le modifiche su singole componenti e ridurre il rischio derivante dagli aggiornamenti e dai conseguenti roll-out.

L'accordo raggiunto con Bassilichi, oltre a sanare le carenze tecniche del prodotto Digital Signage senza costi aggiuntivi, permette a BMPS di recuperare i danni subiti e, nello stesso tempo, irrobustire e sviluppare la relazione commerciale con il gruppo Nexi.

Attività di rafforzamento della sicurezza informatica

Il Consorzio ha utilizzato le informazioni acquisite durante l'analisi dell'incidente e l'approfondimento Audit per integrare nel proprio piano di implementazione della sicurezza informatica "Monte più Sicuro" un insieme di ulteriori attività che complessivamente ne rafforzano l'impianto:

- revisione di tutte le utenze con diritti di amministrazione sui sistemi della Banca;
- attivazione di un processo trimestrale volto alla verifica dei privilegi autorizzativi utilizzati da tutte le componenti applicative/tecnologiche in produzione;
- rafforzamento del processo di Verifica Architetturale e di Sicurezza (tra cui: esplicitazione dei requisiti mandatori di sicurezza nel corpus dei requisiti progettuali) per verificare e garantire "ex ante" che tutte le nuove componenti applicative/tecnologiche siano progettate per avere tutti e solo i privilegi autorizzativi strettamente necessari all'operatività ed essere implementate coerentemente agli standard di Sicurezza COG;
- introduzione di specifici controlli nel processo di sviluppo e test del software atti a garantire "prima del rilascio in produzione" la qualità e la sicurezza del codice sorgente delle componenti applicative classificate come critiche di concerto con le funzioni Rischi e Sicurezza della Capogruppo.

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

3. CONDIVISIONI/PARERI PREVENTIVI

La presente comunicazione sarà preventivamente esaminata dal Comitato Rischi.

Allegato File: Allegato 1 Relazione Direzione Chief Audit Executive su incidente ATM.pdf
Allegato File: Allegato 2 Accordo commerciale per MPS modulo base .pdf

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

DIREZIONE CHIEF AUDIT EXECUTIVE

Siena, 04/05/2018

SERVIZIO IT & OPERATIONAL AUDIT

Oggetto: ***Incidente ATM del giorno 19 febbraio 2018***

1 Executive Summary

In data 19 Febbraio u.s. si è manifestata un'anomalia tecnica sul parco ATM della Banca che causava il blocco operativo delle macchine.

La scrivente Funzione di Audit, che da qualche giorno aveva avviato una revisione ordinaria sulla gestione degli ATM, prevista nel Piano di Audit 2018, ha svolto un approfondimento sulle cause dell'incidente e sulla dinamica degli eventi.

Le strutture operative hanno da subito identificato come causa dell'incidente un intervento tecnico effettuato dal fornitore Fabbrica Digitale S.r.L., a cui Bassilichi, ditta appaltatrice per il Consorzio Operativo Gruppo Montepaschi (di seguito COG) del servizio di Digital Signage[1], ha subappaltato la fornitura del software a supporto (Xuniplay).

Tale intervento, mirato a rimuovere un file di log che generava problemi di spazio sul disco fisso degli ATM, è stato effettuato mediante la distribuzione di un file di configurazione in cui era presente un errore sintattico ed ha causato, sulle sole macchine con sistema operativo Windows XP Embedded (n. 1.456 su 2.758), la cancellazione di alcuni file di sistema.

Gli ATM continuavano regolarmente ad erogare il servizio, ma, in caso di riavvio, la macchina si bloccava, richiedendo un intervento tecnico on-site per un nuovo set up. Lo stesso file non ha prodotto invece anomalie sulle macchine con sistema Windows 7.

Il COG e le Funzioni di Governo degli ATM[2] di Banca MPS hanno cooperato al fine di individuare la problematica, ridurne al minimo l'impatto e approntare idonee contromisure nei giorni successivi all'evento.

Da subito sono state attuate tutte le misure, tecniche e organizzative, necessarie ad impedire il riavvio programmato degli ATM, riuscendo così a stabilizzare il numero di quelli bloccati. Il picco massimo di disservizio si è raggiunto il 25 febbraio con 430 macchine ferme (15% del totale).

Nei giorni successivi si è quindi proceduto al ripristino delle macchine impattate. In particolare:

- per quelle ancora attive è stata approntata una procedura di ripristino da remoto dei file di sistema che erano stati erroneamente cancellati[3] (66,2%);
- per le macchine spente si è invece dovuto ricorrere ad un intervento on site.

Le attività di ripristino complessive sono terminate il giorno 8/3/2018.

Dagli approfondimenti svolti successivamente all'incidente è stato appurato che la distribuzione del file di configurazione è stata svolta da Fabbrica Digitale, sulla base di una segnalazione da parte del fornitore Tas

[1] Digital Signage è una forma di comunicazione di prossimità sul punto vendita o in spazi pubblici aperti o all'interno di edifici, anche nota in Italia come **segnaletica digitale**, *videoposter* o cartellonistica digitale, i cui contenuti vengono mostrati ai destinatari attraverso schermi elettronici o videoproiettori appositamente sistemati in luoghi pubblici.

[2] Area Acquisti, Cost Management e Logistica – Servizio Cash Management, Atm e Logistica.

[3] La procedura ha reinstallato completamente la macchina a una versione precedente in cui non era presente il software Xuniplay.

Group (società fornitrice del software di base installato sugli apparati ATM) che evidenziava la saturazione dello spazio disco a causa dell'incremento delle dimensioni del log del prodotto Xuniplay.

Tale attività è stata svolta da Fabbrica Digitale senza il rispetto delle fasi autorizzative previste dal processo di Change Management (che governa le modifiche del software in ambiente di produzione), nonostante il Consorzio avesse più volte esplicitato al fornitore tale vincolo, peraltro già rispettato nelle precedenti occasioni.

Inoltre, l'operatore di Fabbrica Digitale ha eseguito le modifiche ricorrendo ad una consolle amministrativa priva di controllo accessi, utilizzando funzionalità di distribuzione di cui il Consorzio non era a conoscenza e che aveva piuttosto chiesto di eliminare.

Si osserva altresì che, nonostante quanto premesso, la cancellazione dei file di sistema che ha determinato il blocco degli ATM non sarebbe comunque stata possibile se alle componenti software installate sulle macchine fossero stati assegnati profili abilitativi circoscritti alle effettive necessità applicative, piuttosto che privilegi di amministratore che, di fatto, rendevano possibile il pieno controllo della macchina. A tal proposito si evidenzia l'assenza in fase progettuale di una dettagliata analisi di sicurezza finalizzata all' "hardening" dei sistemi.

Il Consorzio ha inviato in data 23 febbraio 2018 alla società Bassilichi, e per conoscenza a Fabbrica Digitale, una contestazione per interruzione di servizio degli ATM, con conseguente sussistenza di colpa estremamente grave da chi aveva posto in essere le attività, riservandosi pertanto di richiedere il risarcimento dei danni connessi.

Lo stesso Consorzio ha avviato tutte le azioni necessarie a mettere in sicurezza il software affinché non si ripresenti un evento analogo.

L'incidente non ha avuto un impatto rilevante sulla disponibilità degli ATM, grazie anche alle attività di remediation messe tempestivamente in atto dalla Banca e dal Consorzio

L'incidente è stato comunicato agli organi apicali ed al CdA della Banca e, in ragione di tale escalation, è stato anche segnalato all'Autorità di Vigilanza in data 26 febbraio 2018.

2 Attività di Verifica

2.1 Overview Tecnologico

Il software Xuniplay è stato introdotto nell'ambito del Digital Signage a fine 2016 per la gestione e diffusione di contenuti relativi alle comunicazioni istituzionali e commerciali della Banca.

Le tipologie di terminali coinvolti nella distribuzione dei contenuti multimediali sono i seguenti:

- Schermi presenti nel salone della filiale o di altre sedi,
- Totem (non ancora attivo),
- ATM,
- Tablet per la firma grafometrica (di prossima attivazione).

Il software Xuniplay è fornito in outsourcing dal fornitore Fabbrica Digitale tramite una piattaforma applicativa e infrastrutturale proprietaria. Questa è costituita da:

- Una componente applicativa centrale, installata su alcuni server presso il data center del Consorzio, finalizzata alla gestione dei palinsesti pubblicitari e alla loro distribuzione sui terminali locali.
- Alcuni programmi, detti agent, installati sui singoli terminali (es: ATM), che comunicano con la componente centrale per la pubblicazione dei contenuti multimediali.

Tali agent agiscono come amministratori locali della macchina e pertanto con pieni diritti sui terminali. Per gli ATM sono utilizzati solo per trasferire i contenuti multimediali, mentre la visualizzazione è affidata al software di base per la gestione degli ATM (Neptune), fornito da Tas Group.

Il personale di Fabbrica Digitale è dotato di un accesso remoto VPN[4] ai server centrali per esigenze di monitoraggio e gestione.

BMPS (in particolare l'Area Comunicazione) dispone di un cruscotto gestionale delle componente applicativa centrale, detto anche di Back Office, con il quale vengono predisposti e veicolati sui terminali i contenuti e le campagne pubblicitarie di Digital Signage.

2.2 Ricostruzione dell'incidente e interventi immediati

All'origine dell'incidente sta la constatazione, da parte di TAS Group[5], che alcuni log del prodotto Xuniplay stavano saturando lo spazio disponibile nei dischi degli ATM, in particolar modo dei modelli più vecchi e quindi con minore capienza.

La soluzione individuata da Fabbrica Digitale è stata la cancellazione dei log più vecchi di 30 giorni, attraverso una modifica della configurazione del software. In data 7 febbraio u.s. Fabbrica Digitale comunica via mail al Consorzio di aver predisposto la suddetta modifica e di averla anche testata con esito positivo.

Nonostante la mancata risposta alla mail, un operatore di Fabbrica Digitale attivava la distribuzione della modifica su tutte le macchine.

Nella mattina del 19 febbraio veniva rilevato il blocco dei primi 96 ATM.

Le prime analisi evidenziavano che per 1.456 ATM, tutti con sistema operativo Windows XP Embedded, su un totale di 2.758 presenti in BMPS, mancava una cartella di sistema denominata "System32". La cancellazione di tali file, avvenuta a fronte della distribuzione del nuovo file di configurazione del software, non pregiudicava nell'immediato le funzionalità degli ATM, ma ne impediva il riavvio qualora, per una qualunque motivo, la macchina fosse stata spenta e riaccesa.

La mattina del 20 febbraio il Consorzio informa l'Area Sicurezza Integrata in merito alla problematica riscontrata sugli ATM.

Alle 8:30 del 22 febbraio le macchine ferme, per riavvio programmato o accidentale, erano 384. Il fenomeno è risultato omogeneamente distribuito su tutte le Aree Territoriali con indisponibilità comprese in un range tra l'11% ed il 20,4%.

Dopo le analisi iniziali della problematica, la Banca ha attuato tutte le misure, tecniche ed organizzative necessarie ad impedire il riavvio programmato degli ATM, riuscendo così a stabilizzare il numero di quelli bloccati.

In particolare:

- è stato inserito un messaggio in bacheca con cui si invitavano le filiali a non riavviare gli apparati;
- è stata rilasciata una procedura ad hoc che evitava lo spegnimento progressivo del parco da bonificare; questo ha evitato spegnimenti fisiologici da giovedì 22 Febbraio, consentendo di stabilizzare il numero degli ATM da riattivare sul posto.

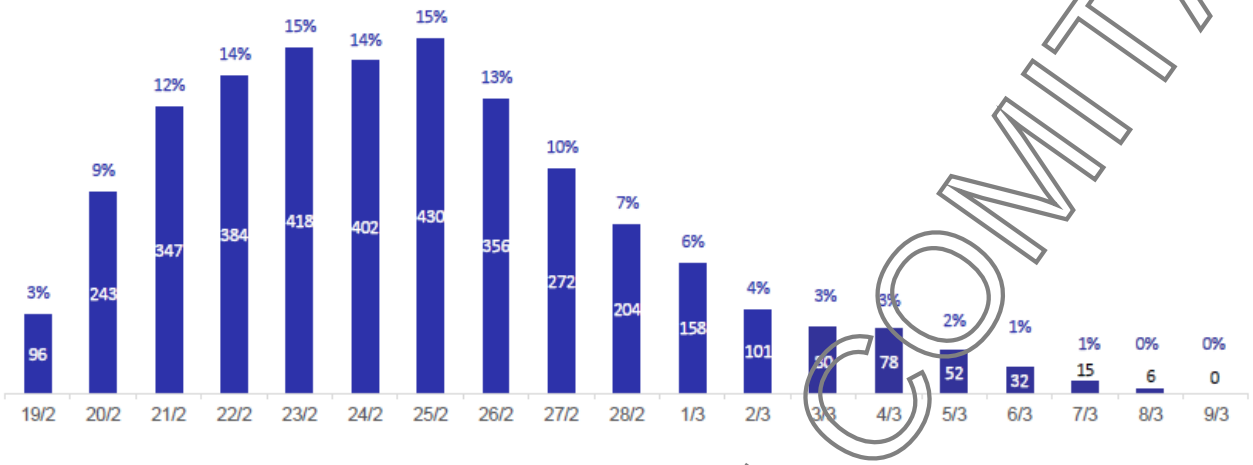
Contemporaneamente è stato definito un piano di interventi per le macchine coinvolte:

- ripristino dei file di sistema rimossi mediante un intervento da remoto su tutte le macchine non ancora bloccate (66,2% di quelle impattate);
- interventi sul posto per ripristinare le macchine già spente non più raggiungibili da remoto: i 384 ATM iniziali e quelli che, nei giorni successivi, si erano bloccate a seguito del fallito tentativo di ripristino effettuato da remoto;
- eliminazione della soluzione di Digital Signage su tutti gli ATM Windows XP Embedded. Sugli ATM con a bordo sistema operativo Windows 7 il software Xuniplay è ancora presente, ma è stato disattivato l'agent che ha generato il problema;

[4] VPN: Virtual Private Network, permette ad un utente di collegarsi da remoto ad una rete privata passando attraverso una rete pubblica (Internet).
[5] TAS – società fornitrice di Neptune, software di base installato sugli apparati ATM

- disabilitazione di tutte le utenze assegnate agli operatori di Fabbrica Digitale per l'accesso ai sistemi del Consorzio.

Le attività di ripristino da remoto si sono concluse in data 25 febbraio, quelle on-site il giorno 8 marzo. Il grafico seguente mostra l'andamento degli ATM fermi a causa dell'incidente.



2.3 Approfondimenti tecnici sulle cause dell'evento

Analizzando il file di log di un ATM con Sistema Operativo Windows XP Embedded si è appurato che la cancellazione dei file del sistema operativo (cartella C:\WINNT\system32) è stata eseguita da un agent, denominato "Device Manager", del software Xunyplay presente sui terminali ATM. L'agent in argomento legge ed esegue le istruzioni presenti nel file di configurazione denominato "configuration.xml" che, tra le altre, contiene indicazioni in merito ai percorsi in cui ricercare i file da cancellare.

È stato pertanto acquisito ed esaminato il file di configurazione in oggetto presente sia nelle macchine con Sistema Operativo Windows 7 che Windows XP Embeded; mentre nel primo caso non sono state riscontrate difformità, nel secondo è stato rilevato un errore sintattico in merito agli attributi associati ad un'istruzione di cancellazione dei file.

La distribuzione sugli ATM del file di configurazione non è avvenuta nell'ambito dei canali standard previsti dal Consorzio[6]. Ciò nonostante che, dalle evidenze raccolte, il fornitore, cui era stato esplicitamente richiesto di inibire tutte le funzionalità di software distribution proprietarie della suite Xuniplay[7], fosse informato e consapevole in merito ai processi e alle procedure da adottare per i rilasci software in ambiente di produzione[8].

La distribuzione della configurazione è stata infatti effettuata ricorrendo ad una consolle di amministrazione[9], nota al Consorzio solo come "data Editor" sui dati di configurazione del Backoffice, tramite la quale era invece possibile inviare o eseguire comandi da remoto, tra cui quelli di aggiornamento ai file di configurazione presenti sui vari terminali. Suddette funzionalità di distribuzione ed esecuzione comandi da remoto non erano note al Consorzio che ne aveva chiesto la totale rimozione. La consolle, inoltre, è risultata accessibile in modalità anonima, ovvero senza necessità di indicare le credenziali di accesso: utente e password.

Si osserva altresì che, nonostante quanto premesso, la cancellazione dei file di sistema che ha determinato il blocco degli ATM non sarebbe comunque stata possibile se alle componenti software installate sulle macchine fossero stati assegnati profili abilitativi circoscritti alle effettive necessità applicative, piuttosto che privilegi di amministratore che, di fatto, rendevano possibile il pieno controllo della macchina.

[6] Il processo standard di Change Management prevede la creazione di una Request for Change - RFC da parte del personale interno del Consorzio, la confezione di un pacchetto in standard DAS e la relativa propagazione sulle macchine tramite software distribution.

[7] Si osserva che in fase progettuale, il fornitore aveva provveduto a modifiche in tal senso intervenendo sull'agent denominato "FdAutoUpdater" che, nella suite Xuniplay, si occupa di scaricare gli aggiornamenti software dai server centrali.

[8] Nel corso del 2017 sono stati effettuati 3 rilasci software sui terminali, tutti in conformità al processo di Change Management definito dal Consorzio.

[9] https://ds.gruppo.mps.local/AutoUpdaterAdmin/

A tal proposito si evidenzia l'assenza in fase progettuale di una dettagliata analisi di sicurezza finalizzata all' "hardening" dei sistemi. Il Consorzio ha comunque dichiarato di aver seguito il progetto Xuniplay con un gruppo di lavoro cui hanno partecipato, nel continuo, anche le funzioni responsabili dell'architettura e della sicurezza dei sistemi informativi.

Fabbrica Digitale ha confermato che, proprio tramite il suddetto pannello di controllo, un suo operatore ha inviato i comandi che hanno aggiornato il file di configurazione sopra citato[10]. Nell'unico log tecnico disponibile non erano comunque individuabili gli utenti che hanno fatto accesso alla consolle.

Fabbrica Digitale ha informato il Consorzio tramite email che le modifiche al file di configurazione erano state da loro testate in ambiente di collaudo con esito positivo, e contestualmente ha richiesto l'autorizzazione a procedere con la distribuzione in ambiente di produzione. Alla suddetta mail di Fabbrica Digitale il Consorzio non ha dato seguito a nessuna risposta.

Dalle successive verifiche da parte del Consorzio sulle macchine di collaudo è risultato che l'anomalia si era generata anche nel corso delle attività di test (i file di sistema erano stati cancellati), pur non manifestandosi in quanto le macchine non erano state riavviate.

Si precisa che al momento della verifica di audit le macchine ATM di collaudo utilizzate per i test erano già state ripristinate più volte, proprio per verificare l'origine del malfunzionamento e per valutare le operazioni correttive da adottare, pertanto non è stato possibile riscontrare sui log le prove svolte e l'autore delle stesse.

2.4 Azioni intraprese per la rimozione delle cause

A seguito dell'incidente, e per evitare il ripetersi di casi analoghi, il Consorzio ha disabilitato tutte le utenze di Fabbrica Digitale con accesso via VPN ai sistemi della Banca ed ha provveduto a rimuovere il software Xuniplay dagli ATM con sistema operativo Windows XP Embedded. Su tutti gli ATM con sistema operativo Windows 7, invece, il software Xuniplay è stato lasciato attivo ma è stato disattivato l'agent Device Manager, coinvolto nell'accaduto.

Con il supporto del fornitore Fabbrica Digitale, in data 4 aprile, è stato aggiunto un sistema di autenticazione alla consolle di amministrazione di Xuniplay, concedendo l'accesso a soli 3 utenti del Consorzio.

E' stato poi avviato uno studio approfondito in merito alle complessive funzionalità dei componenti software che costituiscono la suite Xuniplay, individuando le seguenti azioni:

- Disattivazione di tutti i processi non utilizzati.
- Definitiva rimozione di tutte le funzionalità di auto aggiornamento del software, riconducendo così ogni tipo di modifica e distribuzione agli standard previsti per il processo di Change Management[11].
- Eliminazione per i processi in essere delle prerogative di amministratore di sistema. E' allo studio l'utilizzo di utenti applicativi con privilegi minimi (utente USER) e, comunque, limitati ad agire solo su specifiche directory. A causa del fatto che uno dei suddetti processi (Autoupdater) è tuttora parte attiva nella fase di aggiornamento del software, il completo raggiungimneto di tale obiettivo è perseguibile solo mediante la rivisitazione del software di cui al punto precedente.
- Divisione tra i vari pacchetti applicativi che compongono il prodotto, in modo da frazionare le modifiche su singole componenti e ridurre il rischio derivante dagli aggiornamenti ed i conseguenti roll-out.
- Suddivisione della suite Xuniplay al fine disporre di pacchetti software distinti in funzione del tipo di dispositivo su cui devono essere installati (ATM, schermi, PC collegati alle tavolette utilizzate per la firma grafometrica), ognuno dei quali presenta rischi specifici.

[10] Su tutte le macchine ATM è installato un agent, denominato FdAutoUpdater, che verifica ogni 15 minuti l'allineamento tra il file di configurazione locale e quello centrale, nel caso di differenze scarica un task di allineamento parametri che determina l'aggiornamento del file di configurazione locale.

[11] Creazione di una Request for Change - RFC, di un pacchetto DAS e propagazione tramite software distribution.

2.5 Verifica impianto contrattuale

Il Contratto per l'acquisto, la configurazione e la manutenzione della piattaforma Digital Signage è stato stipulato dal Consorzio e da Bassilichi in data 20/6/2017, con decorrenza dal 1/1/2018 e durata di tre anni con possibilità di rinnovo per altri due. Il corrispettivo previsto per i tre anni è di € 688.000,00.

La regolamentazione dei cambiamenti software è normata nei seguenti documenti che costituiscono parte integrante dell'impianto contrattuale:

- l'allegato 2 "Documento di proposta tecnica Digital Signage per MPS", che prevede, tra le attività a carico del Committente, quella di *Change Management*.
- l'allegato 3 "Condizioni Generali di Contratto del Consorzio Operativo Gruppo Montepaschi" (ver. 8) che, all' Art. 12 Sicurezza, prevede l'impegno del fornitore al rispetto della policy del Consorzio e del Gruppo Montepaschi volta per volta vigente in tema di sicurezza fisica, logica e organizzativa.

L'allegato 3 regola, tra le altre condizioni, anche l'eventuale subappalto a terzi, che deve essere preventivamente autorizzato dal Committente. In data 3/4/2017 Bassilichi ha inoltrato la richiesta di autorizzazione al subappalto a Fabbrica Digitale Srl per la fornitura e gestione della piattaforma Xuniplay, che è stata regolarmente accettata dal COG.

2.6 Comunicazioni alle Autorità di Vigilanza

Il 20/02/2018 il Consorzio ha informato l'Area Sicurezza Integrata in merito alla problematica riscontrata sugli ATM.

Il 23/02/2018 è stata aperta (tramite e-mail) la segnalazione di Major Incident n. INC000003616875 che ha impattato l'ambito dell'Area Acquisti, Cost Management e Logistica (inizio incidente 19/02/2018).

L'evento è stato portato a conoscenza del Comitato Gravi Incidenti (CGI) nelle sessioni del 23 marzo, Nel discutere gli impatti dell'incidente, il Comitato ha preso atto che il disservizio si attestava intorno al 20% di ATM non operanti.

Sulla base di suddette quantificazioni, e nella consapevolezza che i presidi adottati avrebbero con tutta probabilità condotto alla risoluzione della situazione senza far registrare peggioramenti sull'indisponibilità totale del servizio, il Comitato ha ritenuto di non dover classificare l'incidente come "grave" e quindi di non effettuare la prevista segnalazione a Banca d'Italia.

Successivamente al Comitato, della situazione è stato informato anche l'Amministratore Delegato, il quale ha richiesto che l'informativa venisse portata anche all'attenzione del Consiglio di Amministrazione.

Alla luce della suddetta escalation informativa, il Comitato Grave Incidenti si è nuovamente riunito nel pomeriggio di lunedì 26 Febbraio e, preso atto delle comunicazioni occorse o in fase di predisposizione, ha ritenuto opportuno rivedere la decisione assunta nella seduta precedente, deliberando la segnalazione dell'incidente a Banca d'Italia, poi prontamente effettuata nella stessa giornata.

3 Conclusioni

Nonostante l'incidente sia stato innescato da un'azione non autorizzata da parte del fornitore Fabbrica Digitale, contravvenendo agli standard in termini di processo di rilascio in produzione, alcune debolezze di architettura e di sicurezza della soluzione hanno permesso il blocco delle macchine.

In particolare:

- La componente centrale della soluzione Xuniplay non avrebbe dovuto distribuire sulle macchine ATM nessun tipo di modifica al software, mentre funzionalità non note del prodotto ne hanno permesso la distribuzione.
- La componente software Xuniplay distribuita sui singoli ATM non avrebbe dovuto avere i permessi operativi per poter cancellare file di sistema, compromettendone il funzionamento.

L'incidente è stato gestito in maniera coordinata, tempestiva ed efficace, ciò che ha permesso di limitare l'impatto sulla Banca. Immediatamente dopo l'incidente sono state avviate tutte le azioni necessarie a mettere in sicurezza il software.

La presente nota verrà inclusa negli esiti dell'Audit in corso sulla gestione degli ATM; sarà comunque anticipata al Collegio Sindacale, all'Amministratore Delegato e al Presidente del Comitato Rischi.

CartaSi | ICBPI

nexi

Monte dei Paschi di Siena S.p.A.
Via Montanini, 82
53100 Siena (SI)
c.a. Dott. Paolo Deibrato

Milano, 22 maggio 2018

Protocollo n. 2018/2452
Oggetto: Accordo Commerciale per MPS – modulo base

Nell'ambito del rapporto di partnership in essere con il vostro Gruppo, basandoci sulle intese condivise nel corso dell'ultimo mese, vi confermiamo la volontà di concordare un accordo commerciale con l'obiettivo di valorizzare e consolidare la relazione in essere.

Tale accordo commerciale è articolato in due componenti, un **modulo base** e un **modulo addizionale**.
Il presente documento formalizza la componente base, nell'assunzione che Nexi e MPS definiranno possibilmente entro il 31/5/2018 anche la componente addizionale che rappresenterà parte integrante di quanto descritto di seguito, a completamento delle iniziative di incentivazione finalizzate a rafforzare gli obiettivi di business.

Il modulo base consiste in un incentivo pari a 70 euro upfront per ogni POS contrattualizzato dalla Rete BMPS a partire dal 1/6/2018 per le prime 5.000 contrattualizzazioni (flusso lordo di nuovi terminali/POS), per un totale massimo complessivo di 350.000,00 euro da corrispondere alla Banca in un'unica soluzione al raggiungimento dell'obiettivo dei 5.000 contratti cui sopra.

Le modalità di contabilizzazione dell'incentivo saranno definite tra le parti in base a quanto già in essere nell'ambito del citato rapporto di partnership, con allocazione su società nell'ambito del perimetro societario del Gruppo Nexi che sarà successivamente definita.

nexi

Nella certezza che vorrete apprezzare la nostra concreta volontà di consolidare ulteriormente il rapporto di stretta collaborazione tra le nostre Aziende, vi preghiamo di restituirci l'originale della presente debitamente sottoscritta per accettazione entro 30 giorni dalla data del documento, per permetterci la corretta allocazione dei contributi in vostro favore.

Un cordiale saluto.

Marco Ferrero
Commercial Division Director

BANCA MONTE DEI PASCHI DI SIENA SPA

PER ACCETTAZIONE
BANCA MONTE DEI PASCHI DI SIENA
PAOLO DEL PRATO
RESP. AREA MERCATI e PRODOTTI RETAIL