最終草稿

NEMA-COCIR-JIRA 承認のために

2004-07-07

ブレークグラス―― ヘルスケアシステムへの非常時アクセスを許すことへのアプローチ

最終的な SPC Approval の日付: 2004-07-07

www.nema.org/medical/spc
Secretariat: NAMA(National Electrical Manufacturers Association)www.nema.org
1300 第 17North 通り、スイート 1847、ロスリン、ヴァージニア 22209 米国
Secretary: Stephen Vastagh Tel: 703-841-3281 Fax: 703-841-3381、電子mail:
ste_vastagh@nema.org

1. 目的と範囲

この白書は時々「ブレークグラス」と呼ばれる簡単な、しかし、有効な非常時アクセス対策について議論します。 ブレークグラスの目的は通常の認証が首尾よくできないし、または適切に働いていない場合で操作者にシステムへの非常時のアクセスを許すことです。システムは医療情報システム(MedIS)とまとめて呼ばれる情報システムと同様に医療のデータ取得装置を含んでいます。

ブレークグラスはそれらを手頃な管理オーバーヘッドで利用可能にすることができる方法で管理された事前準備された「非常時」ユーザアカウントに基づいています。 この解決方法は、アクセスが承諾される前に、ユーザ名やパスワードなどのように操作者がログインするのを必要とする広範囲な既存のシステムと構造において使用することができます。

ブレークグラスは、長い年月をかけて検証されて、強健であり、追加自動化された技術を必要としません。 それは明確に救急時をカバーするためのものあり、ヘルプデスクの代替として使用するべきではありません。

この白書は MedIS とヘルスケア IT 経営幹部を対象にします。 SPC は、彼らが非常時のアクセスシステムを開発するのを示します、この紙で説明された非常時のアクセス能力を考慮に入れて。

2. 序論

歴史的に、ユーザの特定と認証無しで、多くの MedIS を使用することができました。 しかしながら、合衆国の Health Insurance Portability ＆ Accountability Act (HIPAA)や、ヨーロッパ連合加盟国における EU Directive95/46/EC などの世界中の規則は、個人特定可能な医療データが、それを認可された個人に対して利用可能にし、保護される必要であると断言しました。

ユーザ認証システムは機密データへのアクセスを制御して、モニターするのに使用される典型的なメカニズムの 1 つです。今日 MedIS で使われているそのような多くのシステムが汎用的情報システムの認証構造に基づいています。 それらは、アクセス制限や他の全てにより、セキュリティ保護するように fali-closed に設計されています。Fail-closed はある産業(例えば、金融、保険、製造、国家安全)においてうまく働きます。それは、認証されたユーザへ、システムにより実現される機能とその中に含まれるデータへのアクセスが、一般的には遅れを引き起こすだけだからです。

ヘルスケにおいては、MedIS へのアクセスの遅れは患者の不快・追加負傷・より悪化を引き起こすかもしれず、患者のケアを中断しそうです。この理由で、 HIPAA が、関係者に対しユーザ特定と認証システムに関する問題によって患者のケアを損なわない事を保障する緊急時対策の実施を要求しています。

3. コンティンジェンシー・プランニング

サイトは、現在、リスクアセスメントを行う必要性を認識して、電力供給停止・火災・浸水など非定常時の出来事への用意をします。 準備には縮退プランを開発して、早めにそれらを練習するのを含んでいるので、状況が起こると、皆は、何をしたらよいかを理解しています。 同様の準備は、正常なユーザ登録名と認証が不可能で、ヘルスケアの適切な供給を危険にさらすかもしれない場合に必要です。 そのような緊急対策案の必要性は HIPAA Security Rule によって要求されています。 そして、それは調和するヨーロッパの法律によっても示されています。

正常な過程が不十分であるとき（例えば、ヘルプデスクが入手できないとき）にだけ、非常時のアクセス対策は使用されるべきです。非常時のアクセスが必要であるかもしれないいくつかのケースは:

A. アカウントの問題:
- 忘れられた Username/パスワード、例えば、長期不在 (病気、休暇) の後。
- Password ロック、例えば、あまりに何回も誤タイプにされたためのロック。
- User Account が無い、例えば、医学的に有能な個人が非常時に施設を補助する。

B。 認証システムの問題:
- 組織全体の Authentication System 停止、例えば、集中認証サーバのダウン。
- スマートカードリーダの停止、例えば、カードまたはリーダの破損。
- 生体認証機能の停止、例えば、リーダの誤動作、生体認証機器の破損。

C。 認可の問題:

非常時の医療の状況は操作者が十分なアクセス権を欠いている場合でも、役目（例えば、事務員が非常時にオーダを入れる）を強引に行います。

認証システムが停止する場合には、ユーザ名/パスワードなどの代替の認証メカニズムがあるはずです。

4. ブレークグラス

ブレークグラスは事前準備された非常時のユーザアカウントに基づいていて、不合理な管理遅れなしですぐに利用可能な状態で、管理されて分配されます。この解決方法は 緊急時対策は簡単で、有効で、信頼すべきというガイドラインに従います。

4.1. アカウントの事前準備

非常時アカウントは、アクセス管理とそれらに関連する監査証跡に対して注意深く考えて、作成されるべきです。「事前準備」の非常時アカウントを作成するとき、サイトの管理プライバシーとセキュリティポリシに調和しなければなりません。 以下の要素が考えられるべきです:

A. ユーザ名が明白であって、重要であるべきである、例えば、emergency001 は、アカウントが通常操作には明らかに不適当であり、監査で際立ちます。
B. パスワードはMedISの制約の中で推測、または破るのが困難であるべきです。 それらは難しくはありません。非常時に、ユーザが問題を持たないことが重要です。
C. アカウントPermissionsはリスクアセスメント結果に基づいて、それらのタスクを実行するのに必要である最小特権、例えば、タスクを実行するために必要な最小のデータと機能への非常時ユーザによるアクセス認可に設定されるべきです。これは見るだけ機能になるかもしれません、ローカルコンソールかネットワークの外からのアクセス禁止、データ取得だけへの制限、または前から有るデータへのアクセス禁止。 非常時の必要性を予期するという困難のため、サイトは、非常時のアカウントへの完全なアクセスを許すこと選ぶかもしれません。
D. アカウント用法の詳細とアカウントを使用している間に実行された仕事の詳細を登録するために利用可能であるなら、監査は可能にされるべきです。 あるシステムが、非常時のアカウントを認識して、システム監査レベルを上げるか、または非常時のアカウントだけの監査ログを増加させるかもしれません。

アカウントの詳細を知っている人々が乱用の源であるかもしれないので、アカウントを作成する人々が監査証跡をレビューしないことを保証するための注意が必要です。 さらに、アカウントと分配手順は、それらが必要であるときに、迅速なアクセスを保証するためにテストされるべきです。

4.2. アカウントの分配

ブレークグラス用アカウントは、タイムリーなアクセスを提供するために慎重に管理される必要があります。 ブレークグラスは、適切で合理的な方法で非常時アカウントの詳細を利用可能にするのを必要とします。 これらの詳細は、印刷されたページ、磁気カード、スマートカードかトークンなどのメディアで提供かもしれません。ブレークグラスアカウントのためのいくつかの分配の可能性は以下があります:

A. ガラスの後ろにキャビネットの中において保ち、そこではアカウントへのアクセスが文字通りガラスを割るのを(消火器かアラームと同様の)必要とします。アカウントが使用されたという明示と、通常時の使用への抑止力があります。
B. 封をした封筒の中に保存し、切られた封はアカウントを使用したこと明白的に指示します。
C. 特定の人々(例えば、担当看護師または施設警備員)だけがアクセスすることができる机の引き出しにロックします;
D. 封をしてナースステーションでモニターの側面にテープで留めて紛失、破損が多くの目に明確にわかるようにします。
E. 非常時宣言に複数人の宣言が要るケースで、1 人の人が組み合わせを知っているか、または 1 人がキャビネットのキーを持ち、他人が部屋の鍵を持ち金庫とキャビネットをロックするケース。

ベストプラクティスは事前準備された非常時アカウントを個人責任の注意に置くでしょう。 この Emergency Account マネージャは、業務時間の間、容易に手があいているだれかと非常時アカウントの感度と優先権を理解している人(例えば、シフトマネージャ、看護婦長またはガードマン)でしょう。分配手順は個人識別が可能な形式での提供を必要とするサインアウト方式を含んでいるでしょう。 アカウントを利用可能にする前にこのアイデンティティを記録するでしょう。 そのような手順に従うのは、非常時のアカウントを使用することで実行された活動が、結局認可された個人に関連しているかもしれないのを保証して、責任を作成して、否認拒否を保証することができます。

4.3. アカウント使用の監視

非常時のアカウントの使用は、慎重に監視される必要があります。 セキュリティ監査を調べるために定義された手順は、非常時アカウントのどんな使用も特定するための通常の方法で、MedIS の中の監査メカニズムが使用されるべきです。 さらに、システムはセキュリティ管理者のために非常時アカウントが活性状態である警告することができます。これらの高められた能力は非常に望ましいのですが、ブレークグラスメカニズムを働かせるための要求ではありません。

MedIS がログイン試行のように簡単なアカウント活動を示す監査証跡を提供することができないなら、ブレークグラスの使用は、実行前に慎重に考えられる必要があります。ブレークグラスはまだ有効なシステムのままで残っているかもしれませんが、それは手動(例えば、紙インク)のログの使用を必要とするでしょう。

サイトポリシはそのようなアカウントの意図された使用と彼らの不適当な使用の結果について説明するべきです。 詳細は、明確に記録されて、関連従業員に伝えられるべきです。 非常時アカウントのすべての使用が密接に監視されるのは、明確であるべきです。

ブレークグラスが、従業員に関連しているのを確実にするためにスタッフの定期的審査と再教育をするべきです。

非常時アカウントの各使用は見直されるべきです。 非常時アカウントの使用が有効であるかもしれませんし、またはそれは悪意のある行為を示すかもしれません。 容認できない使用は、記録されて行動をとられる必要があります。 頻繁な使用は正常なユーザ認証メカニズムに関する問題を示すかもしれません。

また、事前準備された非常時アカウントのこの定期的な監視は、それが働きその使用は検出可能であることを保証するいくつかを活動をさせることを含むべきです。 これは、火災報知機をテストして本当の非常時に働くのを確実しているのと同様です。

4.4. アカウント使用後のクリーンアップ

非常時アカウントが使用された後にクリーンアップするための手順が確立されるべきです。 以下の記述を考えてください:

A. パスワードが知られているので再使用を防ぐために使用された非常時のアカウントを、無効にするか、または削除してください。 MedIS は最初の使用か、8 時間か 1 日などの選択可能な期間に、自動的に非常時アカウントを非活性化することができるかもしれません。 非常時の使用の期間、アカウントを無効にするのを避けてください。
B. 取得されたデータを補正し、適切な操作者の名前を反映させるため、監査してください。
C. 適切であるなら「開示ログ」におけるエントリーをしてください。
D. サイトポリシに従って、データ取得かデータアクセスを含んだ活動をレビューしてください。
E. 非常時アカウント手順と操作が効果的に働いたかどうかを決定し、必要なら調整してください。
F. 今後のブレークグラス使用のための新アカウントを作成して、分配してください。新しいパスワードを中古の非常時のアカウントに割り当てるのはローカルのセキュリティポリシの下で適切でないかもしれません。

同じアカウントがマルチ配線ポイントから利用可能であるなら、アカウントのモニターとクリーンアップは複雑であるかもしれません。 1 つの位置だけでそれぞれのアカウントの詳細を利用可能にすることによって、これを避けることができます。

5. 結論

患者データへの非常時アクセスのソリューションを実現するために、多くのもっともな理由があります。 患者管理は最高レベルです。 HIPAA Security Rule、対応するヨーロッパの法律、および日本のプライバシー規則はすべて、非常時のアクセス対策を促進します。 この白書で説明されたブレークグラスは、すべて患者のためにヘルスケアの連続した有用性を確実にしている間、既存の医療のシステムで実行するのが簡単であり、実際にはどんなユーザ認証システムにも適合させることができて、患者プライバシーを保護して、許容できるユーザ責任を提供することができます。 新しいシステム設計に、自動化された解決策は利用可能であるかもしれませんが、ブレークグラスは合理的で、適切で、どんなヘルスケア組織でも既存システムに費用効率がよく立証された、強健なメカニズムです。