

عنوان البحث

دور إدارة المخاطر واستمرارية أعمالها في مراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة
في المنظومات الحكومية والأهلية

إعداد الطالب/

مشاري بن عبد المحسن بن محمد بن سلوم

إشراف/

الدكتورة أسماء أبو عنزه

العام الدراسي:

2024

مقدمة:

استمرارية الأعمال التقنية هي مجموعة من الخطط والإجراءات التي تضمن استمرارية تشغيل الأنظمة التقنية والبيانات والبرامج الحيوية للمنظومة في حالات الطوارئ أو الانقطاعات المفاجئة. تشمل هذه الطوارئ الكوارث الطبيعية، الهجمات السيبرانية، الأعطال التقنية، أو أي حدث غير متوقع يمكن أن يؤثر على العمليات اليومية. يجب تفعيل دور إدارة المخاطر في مراكز البيانات لضمان استمرارية أعمالها وحماية بياناتها من الهجمات السيبرانية التي تشكل خطراً على البيانات الحساسة. تشمل ذلك تقييم المخاطر، وتطوير استراتيجيات للتعامل معها، وضمان توافر البيانات بشكل آمن وسري. استمرارية الأعمال التقنية تعني الحفاظ على توافر واستمرارية الأنظمة والتقنيات الحاسوبية الحيوية للمنظومة. حيث تشمل هذه الجوانب تخطيط وتنفيذ استراتيجيات وإجراءات لضمان استمرارية الأنظمة والبيانات والبرامج التقنية الأساسية للمنظومة في حالات الطوارئ أو الكوارث الطبيعية.

في ظل التقدم التكنولوجي المتسارع وازدياد اعتماد المؤسسات الحكومية والخاصة على تقنية المعلومات، أصبحت مراكز البيانات محور أساسي لعمليات الأعمال والخدمات الحيوية. ومع ذلك، فإن هذه المراكز تواجه تهديدات متزايدة من الهجمات السيبرانية وفقد البيانات الحساسة، مما يشكل خطراً كبيراً على استمرارية الأعمال والسمعة المؤسسية.

في هذا السياق، تبرز أهمية إدارة المخاطر واستمرارية الأعمال كأدوات فعالة للتصدي لهذه التحديات في مراكز البيانات. إدارة المخاطر تسمح بتحديد وتقييم المخاطر المحتملة وتطوير خطط للتخفيف منها، بينما تضمن استمرارية الأعمال قدرة المؤسسة على الاستجابة والتعافي من أي حوادث أو كوارث تؤثر على عملياتها. يهدف هذا البحث إلى استكشاف دور إدارة المخاطر واستمرارية الأعمال في تعزيز أمن وحماية مراكز البيانات في القطاعين الحكومي والأهلي. سوف يتناول البحث الممارسات والتقنيات المتبعة في هذا المجال، والتحديات التي تواجه تطبيقها، بالإضافة إلى التوصيات والسبل الكفيلة بتعزيز قدرة هذه المراكز على مواجهة التهديدات السيبرانية والحفاظ على سرية ونزاهة البيانات الحساسة.

مشكلة الدراسة:

مراكز البيانات هي مرافق تخزين تستضيف أنظمة الحوسبة والشبكات التي تدعم أنشطة الأعمال الرقمية. إدارة المخاطر في مراكز البيانات وكيفية تحليلها والتخطيط للتعامل معها بشكل آمن و يشمل ذلك تحديد المخاطر، وتقييمها. لتأثير المخاطر على استمرارية العمل وسلامة البيانات. فقدان البيانات أو توقف الخدمة يمكن أن يؤدي إلى خسائر مالية كبيرة وتأثير سلبي على سمعة المنظومة. تواجه المنظومات الحكومية والأهلية تحديات كبيرة في حماية مراكز البيانات الخاصة بها من الهجمات السيبرانية المتزايدة والمعقدة. تكمن مشكلة الدراسة في تحديد الفجوات الأمنية الحالية في هذه المنظومات، وتقييم مدى فعالية الإجراءات والتقنيات المستخدمة في إدارة وحماية مراكز البيانات من التهديدات السيبرانية. كما تسعى الدراسة إلى فهم العوامل التي تؤثر على قدرة هذه المنظومات في التصدي للهجمات، وتقديم حلول مبتكرة لتعزيز مستوى الأمان وضمان استمرارية الأعمال.

1. *تحديد وتقييم المخاطر*: يعتبر تحديد وتقييم المخاطر المحتملة التي يمكن أن تؤثر على مراكز البيانات مهمة صعبة بسبب التغيرات المستمرة في التهديدات السيبرانية والتقنيات المستخدمة. البحث في كيفية تطوير نماذج تقييم مخاطر فعالة ومحدثة يُعد محوري.

2. *تصميم استراتيجيات استمرارية الأعمال*: تطوير خطط استمرارية الأعمال التي تضمن استعادة البيانات واستمرارية الخدمات بعد حدوث هجمة سيبرانية أو

أي نوع من الانقطاعات. تحديد أفضل الممارسات والحلول التقنية لضمان الاستجابة السريعة والفعالة هو تحدٍ بحثي.

3. *التكامل بين الأمان السيبراني واستمرارية الأعمال*: غالباً ما تُدار المخاطر واستمرارية الأعمال كعمليتين منفصلتين. البحث في كيفية تكامل هاتين العمليتين بشكل فعال لتحقيق حماية أفضل يمثل تحدياً كبيراً.

4. *الامتثال للتشريعات والمعايير*: مراكز البيانات، خاصة في القطاعات الحكومية والأهلية، يجب أن تلتزم بمجموعة معقدة من القوانين والمعايير. البحث في كيفية تحقيق هذا الامتثال بكفاءة مع الحفاظ على مستويات عالية من الأمان واستمرارية الأعمال هو مجال حيوي.

5. *تحديات التقنية والبنية التحتية*: تطوير وصيانة بنية تحتية قوية لمراكز البيانات يتطلب استثمارات كبيرة وبحثاً مستمراً في التقنيات الجديدة. البحث في كيفية تحسين هذه البنية لتحمل الهجمات وضمان أعلى مستويات الأداء والأمان هو أيضاً تحدي بحثي.

6. *التدريب والوعي الأمني*: غالباً ما يتم إغفال أهمية التدريب ورفع وعي الموظفين بأمان المعلومات. البحث في أفضل الطرق لتدريب الموظفين وتحسين وعيهم بالمخاطر وكيفية التعامل معها يعد جزءاً لا يتجزأ من تعزيز الأمان في مراكز البيانات.

تكمّن العديد من المؤثرات المعلومة والغير معلومة التي بدورها تشكل اخطر
الرئيسي في مراكز البيانات ومن أهمها عدم الالتزام الكامل بالمعايير والأنظمة
الخاصة بها والتي من شأنها ان تكون اول أبواب الخطر.

من ضمن المعايير المهمة والغير ملتزم بها في كثير من الجهات هو النطاق الجغرافي
لمراكز البيانات حيث أنه من الواجب ان تكون في المدن الصحراوية تحت الأرض
وفي المدن الساحلية يتوجب وضعها اعلى من مستوى سطح البحر.

أهمية الدراسة:

إدارة المخاطر في مراكز البيانات تعد من العوامل الحيوية التي تضمن استمرارية العمل وحماية البيانات الحيوية. مع تزايد الاعتماد على التقنيات الجديدة والبيانات، أصبحت مراكز البيانات هدفاً رئيسياً للهجمات السيبرانية والكوارث الطبيعية والمشاكل التقنية. لذا، فإن تنفيذ استراتيجيات فعالة لإدارة المخاطر يمكن أن يقلل من تأثير هذه التهديدات ويحافظ على سلامة البيانات واستمرارية أعمال المنظومة.

- تحديد المخاطر: بتحديد المخاطر المحتملة. يمكن أن تشمل هذه المخاطر الهجمات السيبرانية، انقطاع التيار الكهربائي، الكوارث الطبيعية، والأخطاء البشرية.
- التقييم: بعد تحديد المخاطر، يتم تقييم مدى تأثير كل خطر على مركز البيانات. يتم ذلك من خلال تحليل الاحتمالية والتأثير المحتمل لكل خطر.
- التخطيط: بعد تقييم المخاطر، يتم وضع خطط للتعامل معها. يمكن أن تشمل هذه الخطط استراتيجيات الوقاية، وخطط الطوارئ، وإجراءات الاستجابة السريعة.
- التنفيذ: يتم تنفيذ الخطط الموضوعة للتعامل مع المخاطر. يشمل ذلك تدريب الموظفين، وتحديث الأنظمة، وتطبيق الإجراءات الوقائية.
- المراقبة والمراجعة: يتم مراقبة فعالية الخطط والإجراءات المتبعة بانتظام، ومراجعتها وتحديثها حسب الحاجة لضمان استمرار فعاليتها.

في العصر الرقمي الحالي، أصبحت مراكز البيانات القلب النابض للمنظومات الحكومية والأهلية، حيث تعتمد عليها المؤسسات بشكل كبير في تخزين ومعالجة البيانات الحساسة. ومع تزايد التهديدات السبرانية، أصبحت إدارة مخاطر هذه المراكز ضرورة ملحة لضمان حماية البيانات واستمرارية الأعمال. يهدف هذا البحث إلى استكشاف استراتيجيات وأساليب إدارة مخاطر مراكز البيانات من الهجمات السبرانية، مع التركيز على المنظومات الحكومية والأهلية. سيتم تسليط الضوء على التحديات التي تواجهها هذه المؤسسات، وأهمية تطوير سياسات أمنية فعالة، وتبني تقنيات حديثة لحماية البنية التحتية الرقمية. من خلال هذا البحث، نسعى إلى تقديم توصيات عملية لتعزيز الأمن السبراني وضمان سلامة البيانات في مواجهة التهديدات المتزايدة.

أهداف الدراسة:

استمرارية الأعمال التقنية هي مجموعة من الخطط والإجراءات التي تضمن استمرارية تشغيل الأنظمة التقنية والبيانات والبرامج الحيوية للمنظومة في حالات الطوارئ أو الانقطاعات المفاجئة. تشمل هذه الطوارئ الكوارث الطبيعية، الهجمات السيبرانية، الأعطال التقنية، أو أي حدث غير متوقع يمكن أن يؤثر على العمليات اليومية

أهمية استمرارية الأعمال التقنية

- حماية البيانات: تضمن استمرارية الأعمال التقنية حماية البيانات الحيوية من فقدان أو التلف.
- تقليل التوقف اعمال المنظومة: تساعد في تقليل فترة التوقف عن العمل، مما يضمن استمرارية العمليات الحيوية للمنظومة بشكل فعال.
- الامتثال التنظيمي: تساعد المؤسسات في الامتثال للمتطلبات القانونية والتنظيمية المتعلقة بحماية البيانات واستمرارية الأعمال.
- الحفاظ على السمعة: تضمن استمرارية الأعمال التقنية الحفاظ على سمعة المؤسسة من خلال تقديم خدمات متواصلة وموثوقة.

- الاستجابة السريعة للطوارئ: تتيح للمؤسسات الاستجابة السريعة والفعالة للطوارئ، مما يقلل من تأثير الأحداث السلبية.

اهداف يلزم تطبيقها:

1. *تحسين فهم المخاطر السيبرانية*: تعزيز القدرة على تحديد، تقييم، وفهم المخاطر السيبرانية التي يمكن أن تؤثر على مراكز البيانات. هذا يشمل تطوير نماذج لتحليل المخاطر بشكل دقيق ومستمر.

2. *تطوير استراتيجيات استمرارية الأعمال*: صياغة وتنفيذ خطط استمرارية الأعمال التي تضمن عدم التوقف الكامل للعمليات في حالة حدوث هجمات سيبرانية أو أي اضطرابات أخرى. الهدف هو تقليل الوقت اللازم لاستعادة الخدمات والمحافظة على الكفاءة التشغيلية.

3. *تكامل الأمان السيبراني مع استمرارية الأعمال*: تعزيز التكامل بين إدارة المخاطر السيبرانية وخطط استمرارية الأعمال لضمان تنفيذ استجابة شاملة ومتكاملة عند الضرورة.

4. *الامتثال للمعايير والتنظيمات*: ضمان أن مراكز البيانات تلتزم بالمعايير والتشريعات المحلية والدولية المتعلقة بالحماية السيبرانية وخصوصية البيانات. الهدف هو تعزيز الثقة في الأنظمة الحكومية والأهلية من خلال الامتثال الصارم.

5. *تحسين البنية التحتية والتقنيات*: استثمار في أحدث التقنيات وتحديث البنية التحتية لتعزيز القدرة على مواجهة التهديدات السيبرانية وتحسين الأداء العام لمراكز البيانات.

6. *تعزيز الوعي والتدريب*: رفع مستوى الوعي والتدريب للموظفين فيما يخص الممارسات الأمنية وإدارة المخاطر، وذلك لتقليل الأخطاء البشرية وتحسين الاستجابة للحوادث.

7. *تقييم وتحسين الممارسات الحالية*: إجراء تقييمات دورية للممارسات والإجراءات الحالية وتحديثها بناء على النتائج لضمان الفعالية المستمرة في حماية البيانات والأنظمة.

ما هو الأثر المترتب عليه أكثر المخاطر في مراكز البيانات؟

تحليل الأثر على الأعمال هو عملية تحديد وتقييم تأثير الانقطاعات المحتملة على العمليات الحيوية للمؤسسة. يساعد هذا التحليل في تحديد الأولويات ووضع استراتيجيات لاستعادة الأنظمة والبيانات بسرعة. يتمثل في تحديد وتقييم المخاطر المحتملة التي قد تؤثر على استمرارية الأعمال التقنية. يشمل ذلك تحليل التهديدات الداخلية والخارجية وتحديد نقاط الضعف في الأنظمة التقنية. يجب وضع خطة الطوارئ واضحة ومنظمة يتم اتباعها في حالة حدوث انقطاع. تشمل هذه الخطة تفاصيل حول كيفية استعادة الأنظمة والبيانات، وتحديد المسؤولين، وتوفير الاتصالات اللازمة. يجب على المختصين التقنيين تنفيذ استراتيجيات فعالة للنسخ الاحتياطي واستعادة البيانات لضمان حماية البيانات الحساسة ويشمل ذلك النسخ الاحتياطي الدوري للبيانات وتخزين النسخ الاحتياطية في مواقع آمنة خارج المنظومة ولا يتم الوصول إليها إلا بموافقة المسؤولين المختصين التقنيين ومسؤولين إدارة المخاطر. على جميع المنظومات تدريب الموظفين على خطط الطوارئ وإجراءات استمرارية الأعمال التقنية. يساعد ذلك في ضمان استجابتهم السريعة والفعالة في حالة حدوث طوارئ.

اختبار خطط استمرارية الأعمال التقنية بانتظام وتحديثها بناءً على التغيرات في البيئة التقنية والمخاطر المحتملة، يساعد ذلك في التأكد من فعالية الخطط وجاهزيتها للتنفيذ في أي وقت قبل.

تطبيق الدراسة وفروضها على عدد من المنشآت الصغيرة والمتوسطة الحكومية والأهلية ويشمل ذلك التأكد من البنى التحتية وخطط الطوارئ لمراكز البيانات في حال حدوث هجمات سيبرانية أو خطأ بشري.

1. *فرضية تطبيق إجراءات أمنية محدثة*: تطبيق إجراءات أمنية محدثة ومتطورة في مراكز البيانات يقلل من احتمالية الهجمات السيبرانية وفقدان البيانات الحساسة في المنظومات الحكومية والأهلية.

2. *فرضية التدريب والوعي*: تحسين مستويات التدريب والوعي الأمني لدى الموظفين يقلل من مخاطر الهجمات السيبرانية والأخطاء البشرية التي قد تؤدي إلى فقدان البيانات.

3. *فرضية الاستثمار في التكنولوجيا*: الاستثمار في تكنولوجيا متقدمة للحماية من الهجمات السيبرانية يعزز من قدرة المنظومة الحكومية والأهلية على حماية بياناتها الحساسة.

4. *فرضية التعاون بين المؤسسات*: التعاون والتنسيق بين المؤسسات الحكومية والأهلية يحسن من كفاءة إدارة المخاطر واستمرارية الأعمال في مواجهة الهجمات السيبرانية.

5. *فرضية الاختبارات الدورية والتقييمات*: إجراء اختبارات دورية وتقييمات للأمن السيبراني يكشف الثغرات ويساعد في تحديث الإجراءات الأمنية بشكل فعال لحماية البيانات.

6. *فرضية التخطيط للطوارئ واستعادة البيانات*: وجود خطط طوارئ مفصلة وفعالة لاستعادة البيانات يقلل من تأثير الهجمات السيبرانية على استمرارية الأعمال.

1. دراسة بعنوان "إطار عمل لإدارة المخاطر في مراكز البيانات لمواجهة الهجمات السيبرانية" نشرت في المجلة الدولية لأمن المعلومات والشبكات عام 2021. تناولت هذه الدراسة تطوير إطار عمل متكامل لتحديد المخاطر وتقييمها والتحكم بها في مراكز البيانات للحد من التأثير السلبي للهجمات السيبرانية.

2. دراسة بعنوان "تعزيز استمرارية الأعمال في مراكز البيانات الحكومية: التحديات والحلول" نشرت في مجلة الحكومة الإلكترونية عام 2020. ركزت هذه الدراسة على التحديات التي تواجه استمرارية الأعمال في المراكز الحكومية وتقديم حلول تقنية وإدارية لضمان استمرارية الخدمات في حالة وقوع أي كوارث أو اختراقات.

3. دراسة بعنوان "أثر الهجمات السيبرانية على البيانات الحساسة في المؤسسات الأهلية: دراسة حالة" نشرت في مجلة أمن تكنولوجيا المعلومات عام 2019. قدمت هذه الدراسة تحليلاً لحالات فقد البيانات الحساسة في بعض المؤسسات الأهلية نتيجة الهجمات السيبرانية وأوصت بتعزيز الجوانب الأمنية والرقابية.

4. دراسة بعنوان "دور إدارة المخاطر في تعزيز استمرارية الأعمال في مراكز البيانات الكبرى" نشرت في مجلة إدارة المخاطر عام 2018. ركزت هذه الدراسة على

الممارسات الفضلى لإدارة المخاطر وربطها باستمرارية الأعمال في المراكز الكبرى
لضمان استمرارية الخدمات والحفاظ على البيانات الحساسة.

1. نظرية إدارة المخاطر:

- التركيز على تحديد المخاطر المحتملة والتقييم الدقيق لآثارها المحتملة.
- وضع استراتيجيات فعالة للتخفيف من المخاطر والتعامل معها.
- ربط إدارة المخاطر باتخاذ القرارات الاستراتيجية في منظمات القطاع الحكومي والأهلي.

2. نظرية استمرارية الأعمال:

- التركيز على ضمان استمرارية الخدمات والعمليات الحيوية في مواجهة الاضطرابات والكوارث.
- تطوير خطط استمرارية الأعمال والتعافي من الكوارث في مراكز البيانات.
- ربط استمرارية الأعمال بتحقيق الأهداف التنظيمية وتقديم الخدمات للمستفيدين.

3. نظرية الأمن السيبراني:

- التركيز على حماية البيانات والأنظمة من الهجمات السيبرانية المتطورة.
- وضع إجراءات وآليات فعالة للكشف عن التهديدات والتصدي لها.
- ربط الأمن السيبراني باستمرارية الأعمال وإدارة المخاطر في مراكز البيانات.

4. نظرية نظم المعلومات:

- التركيز على دور تكنولوجيا المعلومات في دعم وتعزيز إدارة المخاطر واستمرارية الأعمال.

- تصميم وتنفيذ أنظمة معلومات آمنة ومرنة في مراكز البيانات.

- ربط نظم المعلومات بالجوانب التنظيمية والإدارية لضمان الاستخدام الأمثل.

1. المنهج الوصفي التحليلي:

- تحليل الوضع الراهن لإدارة المخاطر واستمرارية الأعمال في مراكز البيانات.
- وصف وتحليل التحديات والتهديدات السيبرانية التي تواجهها هذه المراكز.
- تقييم الممارسات الحالية والآثار المترتبة على فقد البيانات الحساسة.

2. المنهج الاستقرائي:

- استقراء الأدبيات والدراسات السابقة ذات الصلة بموضوع البحث.
- استخلاص الدروس المستفادة والممارسات الناجحة من الحالات المماثلة.
- بناء إطار مفاهيمي شامل لدور إدارة المخاطر واستمرارية الأعمال.

3. المنهج الوثائقي:

- تحليل السياسات والتشريعات المنظمة لأمن المعلومات والاستمرارية في القطاعين.
- دراسة التقارير والإحصائيات الرسمية المتعلقة بالهجمات السيبرانية وفقد البيانات.
- استعراض الوثائق والإرشادات الفنية الصادرة عن الجهات المعنية.

4. المنهج المسحي:

- إجراء مسح ميداني لعينة من مراكز البيانات في القطاعين الحكومي والأهلي.
- جمع البيانات والمعلومات من خلال استبيانات وملاحظات ومقابلات.
- تحليل البيانات الكمية والنوعية لاستخلاص النتائج والتوصيات.

1. الاستبيان:

- تصميم استبيان شامل لجمع البيانات من مديري مراكز البيانات والأفراد المعنيين.
- تغطية محاور رئيسية مثل سياسات الأمن السيبراني، إدارة المخاطر، خطط الاستمرارية، وآليات الاستجابة للحوادث.
- تحليل النتائج الكمية والنوعية للاستبيان باستخدام أساليب إحصائية متقدمة.

2. المقابلات المتعمقة:

- إجراء مقابلات شبه منظمة مع خبراء وقادة في مجال أمن المعلومات والاستمرارية.
- استكشاف التحديات والممارسات الناجحة بشكل تفصيلي من وجهة نظر المختصين.
- تسجيل وتحليل البيانات النوعية المستقاة من المقابلات.

3. ورش العمل وحلقات النقاش:

- تنظيم ورش عمل وحلقات نقاش تفاعلية مع المسؤولين في مراكز البيانات.

- مناقشة القضايا الرئيسية وتبادل الخبرات والأفكار لتطوير الحلول المناسبة.
- توثيق المناقشات وتحليل المخرجات والتوصيات الناتجة.

4. تحليل الوثائق والسجلات:

- مراجعة السياسات والإجراءات الداخلية لإدارة المخاطر واستمرارية الأعمال.
- فحص سجلات الحوادث السيبرانية وإجراءات الاستجابة والتعافي.
- تحليل التقارير والإحصائيات الرسمية المتعلقة بالهجمات وفقد البيانات.

5. المحاكاة والاختبارات:

- إجراء تمارين محاكاة لسيناريوهات الهجمات السيبرانية وانقطاع الخدمات.
- اختبار خطط الاستمرارية والاستعادة من الكوارث في مراكز البيانات.
- تقييم مدى جاهزية المنظمات وفعالية الإجراءات التي يتم اتخاذها.

1. النطاق الجغرافي:

- التركيز على مراكز البيانات في المنظومة الحكومية والأهلية ضمن حدود دولة معينة أو منطقة جغرافية محددة.

- قد يتم توسيع النطاق الجغرافي إلى مستوى إقليمي أو دولي إذا كان الهدف المقارنة بين الممارسات في مختلف الدول.

2. القطاعات المستهدفة:

- التركيز على قطاعات حكومية رئيسية مثل الصحة، التعليم، الأمن، الخدمات العامة.

- دراسة قطاعات أهلية مهمة مثل المؤسسات المالية، الشركات الكبرى، الجهات الصحية والتعليمية الخاصة.

- قد يتم توسيع نطاق القطاعات حسب أهمية البيانات المعالجة وحساسيتها.

3. حجم المنظمات:

- التركيز على مراكز البيانات في المنظمات الكبرى والمتوسطة الحجم.

- قد يتم تضمين بعض المنظمات الصغيرة إذا كانت تمثل نسبة كبيرة من القطاع.

4. متطلبات الأمان والاستمرارية:

- التركيز على المنظمات التي تتطلب مستويات عالية من الأمان السيبراني والاستمرارية في الأعمال.
- قد يتم استبعاد بعض المنظمات ذات متطلبات أمنية أقل أو التي لا تتعامل مع بيانات حساسة.

5. الفترة الزمنية:

- التركيز على الفترة الزمنية الحالية أو خلال السنوات الأخيرة.
- قد يتم توسيع الفترة الزمنية للمقارنة بين الممارسات الحالية والسابقة.

1. "مراكز البيانات: تصميماتها وإدارتها وتشغيلها" - محمد الشريف
2. "إدارة مراكز البيانات: مبادئ وممارسات" - أحمد سالم
3. "تصميم وتخطيط مراكز البيانات" - خالد الحسيني
4. "الحلول الأمنية لمراكز البيانات" - سامي البكري
5. "الكفاءة الطاقية لمراكز البيانات" - محمد البلوشي